INSIDE IT

Das Portal für IT-Verantwortliche

PRESENTS

Layer 2 Encryptors for Metro and Carrier Ethernet, MPLS and IP

Market Overview Ethernet-Encryptors (Point-to-Point and Multipoint)

Short Version

Version 7.1, May 9 2022

www.uebermeister.com
cjaggi@uebermeister.com

ISBN: 978-3-9525012-1-4

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION

CHAPTER 2: MARKET OVERVIEW

Chapter 1: Introduction

1. Encryption Layer and Security

Ethernet is playing a rapidly increasing role for connecting sites. Metro and Carrier Ethernet establish a standard for metropolitan and wide area networks that is situated on layer 2 of the OSI network model. This is one layer below IP, the Internet protocol, which is located on layer 3. On the customer side, Carrier Ethernet has substantial operational advantages over MPLS and is also advantageous in terms of cost.

Encryption Layer	Usage Scenario and Protection
Layer 3: Network Layer (IP)	Remote Access, End-to-End Site-to-Site Network, End-to-End, multi-hop Multi-Site Network, End-to-End, multi-hop L3 VPN
Layer 2: Data Link Layer (Ethernet)	Hop-to-Hop Network, End-to-End (direct Link) Site-to-Site Network, End-to-End, multi-hop Multi-Site Network, End-to-End, multi-hop L2 VPN
Layer 1: Physical Layer	Hop-to-Hop (direct link)

Network encryption provides most efficiency and security if it takes place at the native layer or below. Encryption below the native layer can limit the flexibility available at the native layer.

The increasing demand for dedicated Layer 2 encryptors has a simple reason: security and efficiency coupled with cost savings. More than 99 percent of network attacks occur at layers 3 to 7. Layer 2 encryption of multi-site traffic - if authenticated encryption is used - provides full protection for the network, including confidentiality, integrity protection, authentication, intrusion detection and intrusion prevention. As a result, the encryptor also serves as a line-rate firewall at network level. For this, all traffic at layer 2, including the control plane, has to be secured at layer 2 by hardware. This is also a prerequisite for ensuring availability. Due to the security, integrity and availability provided, there is a growing number of customers for such solutions, including some with over 900 Layer 2 encryptors in 24/7/365 use.
In addition to Ethernet, several vendors now support bridge mode encryption for IP networks.

The most appropriate network encryption for a network is determined by the network used. Different customers have different networks. You can find out how to choose the most suitable network here:

https://my.ipspace.net/bin/list?id=ChooseVPN#HYBRID
https://my.ipspace.net/bin/list?id=Design#2022_01

2. Different Approaches

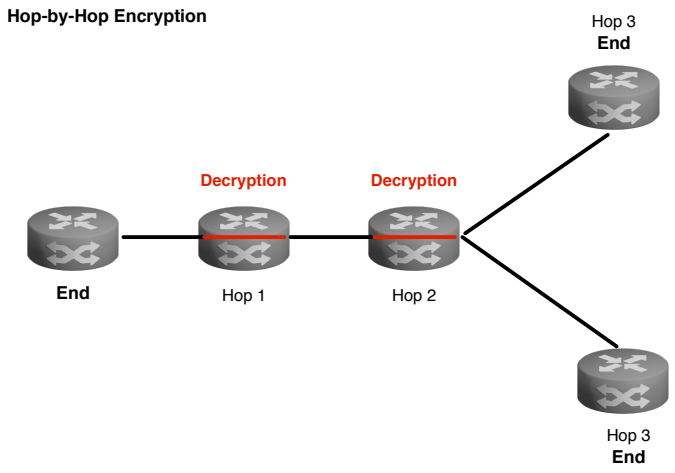
For network encryption there are different approaches and practices. They have a direct impact on the application scenarios supported and the security level provided by a solution.

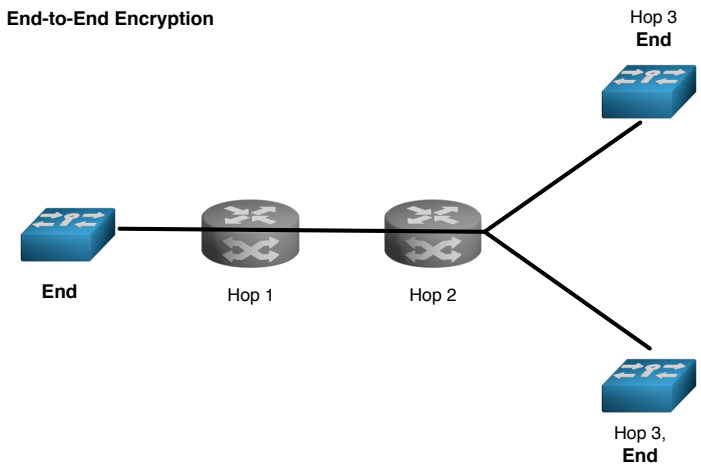
There are different possibilities to encrypt Ethernet networks. It can be done at layer 1, layer 2 and layer 3. It is most efficient at layer 1 and layer 2, and most flexible at layer 2 and layer 3. The optimal combination of efficiency and flexibility is provided by Ethernet encryption at layer 2. Even at layer 2 there are different basic approaches.

2.1. Hop-by-Hop vs. End-to-End

For securing the connection between sites, an end-to-end encryption is the preferred approach, as a hop-by-hop encryption only works in a limited number of scenarios.

A hop-by-hop encryption is an encryption between two nodes that are one hop apart. At each hop the data is decrypted, processed in unencrypted form, re-encrypted and sent to the next hop. End-to-end encryption works differently: The data remains encrypted and secure during the entire transmission between sender and receiver.





In a local area network (LAN) a hop-by-hop encryption can be preferable, but in a MAN or WAN environment it should only be considered as an option if the next hop is also the end-point of the connection. The usage scenario and the flexibility of hop-by-hop encryption solutions are severely limited. Therefore, this market overview focuses on solutions that provide end-to-end security.

2.2. Dedicated vs. Integrated

It is simpler to optimize and secure a dedicated appliance for a specific scope of functions. Integrated solutions tend to come at a lower price and offer less functionality and less security. For Ethernet encryption, nearly all integrated solutions are based on LAN-oriented MACSec, whereas dedicated appliances offer security and functionality that is optimized for the use in MAN and WAN environments. The requirements for MAN and WAN encryption differ quite substantially from the requirements for a LAN encryption, be that in terms of network support or be that in terms of security. Dedicated solutions developed specifically for the protection of Carrier Ethernet networks tend to be better suited than integrated MACSec-based solutions as they have been engineered for the increased network and security requirements of MANs and WANs.

Dedicated solutions designed specifically for the protection of Carrier Ethernet networks are generally better suited than MACSec-based integrated solutions, as they are designed from the outset to meet the increased network and security requirements of MANs and WANs. Dedicated devices based on MACSec have also been available for a few years. However, they use IEEE 802.1AEcg specifications developed by NSA and IEEE and FPGAs instead of ASICs. These devices can handle more Carrier Ethernet scenarios, but fall well short of most purpose-optimized devices in terms of network support, functionality, security, and, in some cases, scalability.

Security solutions for WANs should be optimized for the specific problems and threat scenarios of WAN and MAN in terms of both functionality and security.

3. Criteria and Coverage

3.1. Criteria

The market overview is structured based on the key criteria that are relevant for making a preselection of products to evaluate:

- Interface/processing capabilities
- Supported networks and usage scenarios
- Platform used (hardware, firmware, key management)
- Encryption standards and processing options
- Encryption and security functionality on the data plane
- Encryption and security functionality on the control plane
- Key management and key system
- Network functionality and additional functionality
- Device management
- Certifications
- Device properties

There are explanations for the different criteria and implementation approaches. Where appropriate and available, links to neutral external information sources are provided.

Different customers often have different requirements. On the network side, they are defined by the characteristics and the usage scenario of the MAN or WAN used. On the security side, they are defined by the required protection level. There are different solution approaches to meet the security and network requirements.

There is no official standard for end-to-end encryption of Carrier Ethernet networks, but there are several widely used solutions that are de facto standards. MACsec is a standard developed for local area networks (LAN) and is a hop-by-hop solution by its basic architecture. It works in some Metro and Carrier Ethernet scenarios, but not in others. There are variations of MACsec that also work with Carrier Ethernet. Different vendors of end-to-end solutions use different approaches at both the control and data planes. As a result, the market offering is quite confusing. This market overview tries to show the different solution approaches. The specifications for MACsec are available from the IEEE. Each approach comes with its own advantages and disadvantages. The usage scenario of the user determines the functionality requirements. The most important evaluation criteria are product functionality, security level and acquisition cost. The product selection has an impact on security, compatibility, efficiency, flexibility and ongoing cost.

At Layer 2, IP can also be encrypted in Bridge Mode. Some vendors support this.

3.2. Coverage

The objective of this market overview is to cover the most relevant vendors and, for those that are less relevant and those that did not want to participate, to provide the reader with the relevant questionnaire to be submitted to the vendor.

Five factors are decisive for market relevance: acceptance in the market, installed base, current sales, technical status of the products and portfolio breadth. Thus, this market overview does not include vendors whose products lack essential security functions such as authenticated encryption, cannot encrypt natively at Layer 2, do not support multipoint, or cannot cover the most common bandwidth scenarios - from 100Mb to 100Gb. Also not included are carrier devices where encryption only takes place after the unencrypted network traffic has been handed over to the carrier. These include Ethernet access devices.

With regard to MACSec, the selection is limited to the functionality of a typical IEEE 802.1AEcg device, since this standard, unlike integrated solutions, relies on customer-supplied appliances in the same way as the NSA's Ethernet Security Specifications (ESS). IEEE 802.1AEcg is part of IEEE 802.1AE-2018, deviates from IEEE 802.1AE MACSec in several areas and defines five different device classes. Contrary to an integrated MACSec solution, IEEE 802.1AEcg-based appliances are dedicated and mostly use FPGAs separated from the network port for encryption. The attack surface of such an appliance is much lower than the attack surface of an integrated solution using an ASIC on the network interface. MACsec 802.1AEdk as the next planned extension, adds a combination of tunnel mode with traffic flow security, but is not expected until 2024.

4. Objective

This market overview is intended to reflect the current and planned market offering of appliances from the perspective of the most relevant vendors in terms of the functionality provided. To this end, it shows various approaches and options for securing a Carrier Ethernet MAN or WAN. Functionality requirements are determined by the customer's deployment scenario, while security requirements are determined by the customer's risk tolerance. Product functionality and security offered, along with acquisition and operating costs, are the most important evaluation criteria for customers. The choice made by the customer has an impact on security, compatibility, efficiency, flexibility and follow-up costs.

This market overview does not make recommendations in terms of vendors and platforms. It does, however, provide information in terms of functionality that is helpful and time-saving for creating an RFI, an RFP and a shortlist for evaluation.

The market overview is one of three documents covering Layer 2 encryptors for Metro and Carrier Ethernet, MPLS and IP. There is an introduction, an evaluation guide and a market overview.

The current documents can be found here:

https://www.uebermeister.com/en/networksecurity/resources

Chapter 2: Market Overview

1. Vendors and Products

This market overview covers all relevant vendors of dedicated layer 2 encryption appliances for commercial customers that support a bandwidth spectrum of 100Mb to 10Gb whose products are available in Europe. The products have to meet current security standards, which excludes products lacking authentication and "Perfect Forward Secrecy (PFS)". Most of the devices have a certification issued by a certification body and have been approved for securing networks transporting classified government and defense data. All of these products are COTS (commercial off-the-shelf) products for government, defense and commercial use.

The reason for the limitation to autonomous devices are higher security, less complexity, and vendor-independence concerning switches and routers. Currently there is not even a secure and versatile integrated solution on the market that would offer Ethernet multipoint encryption for multi-hop networks.

Below, the alphabetical list of the most relevant vendors and the IEEE standards for LAN and MAN in this space:

Atmedia
(http://www.atmedia.de/en/index.html)

IDQuantique
(http://www.idquantique.com)

Rohde & Schwarz Cybersecurity
(https://www.rohde-schwarz.com/products/cybersecurity/network-encryptors/rs-sitline-eth_63493-659340.html)
(https://www.rohde-schwarz.com/products/cybersecurity/network-encryptors/rs-sitline-ip_63493-617133.html)

Secunet
(http://www.secunet.com/en/topics-solutions/high-security/sina/sina-l2-box/)

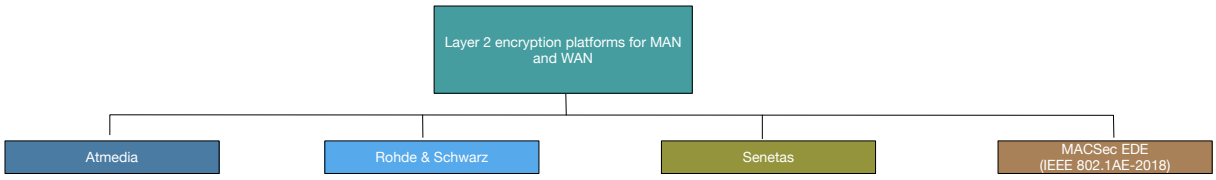
Securosys
(https://www.securosys.ch/layer-2-encryptor-centurion)

Senetas
(http://www.senetas.com)

Thales
(https://cpl.thalesgroup.com/encryption/data-in-motion)

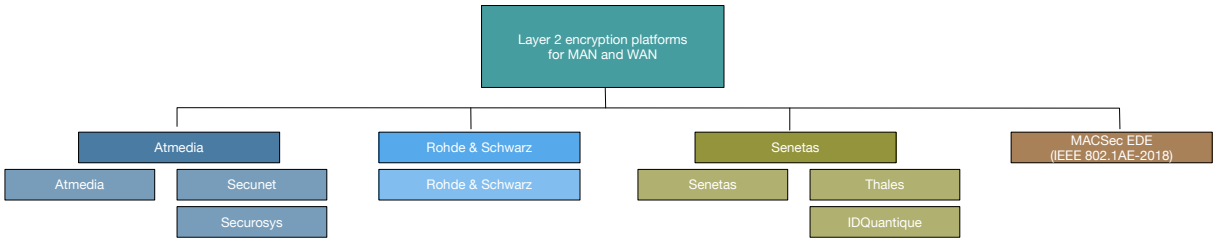
IEEE MACsec EDE
https://standards.ieee.org/ieee/802.1AEcg/5968/
https://standards.ieee.org/ieee/802.1X/7345/

The predominant offers available on the market are based on established platforms:



In the five years since the last market overview, there have been shifts in the market, mainly due to the acquisition of Gemalto by Thales. A large proportion of Thales E-Security products have been replaced by Gemalto/Safenet products. This also affected the Thales Datacryptor products. Since these are built on the Atmedia platform, customers of Thales Datacryptor Ethernet or the 5000 series can upgrade their firmware at Atmedia or a vendor that uses the Atmedia platform. This brings them up to date with the latest technology. Existing service contracts can also be transferred away from Thales, especially since Thales can no longer provide the service.
ViaSat has concentrated its focus on the government and military market and only serves the commercial market opportunistically. Therefore, a generic MACSec EDE profile is used in this market overview.

The following diagram shows the platforms the different vendor's products are based on.



The common denominator of the products is mainly limited to the fact that all carriers can encrypt Ethernet networks natively and authenticated. Except for the use of AES-GCM, all platforms do this differently, and network support is also strongly platform-dependent. Not only the security requirements, but also the networks are constantly evolving due to new technologies, changing customer requirements and new carrier offerings. FPGA- and CPU-based encryptors can be adapted to new security and network requirements via firmware or software updates. The greater the flexibility of an encryptor, the higher the number of supported deployment scenarios.

Below is a detailed breakdown of the most relevant properties and functionalities. The particular requirements profile decides which products can be considered.

2. Network Standards and Platforms

2.1. Ethernet Interface and Data Throughput

The Ethernet network standard supported by a product determines the theoretical throughput of the encryptor. The relevant standards for Ethernet today are the IEEE 802.3 standards 10Mbit Ethernet, 100Mb/s Ethernet, 1Gb/s Ethernet, 10Gb/s, 25Gb/s, 40Gb/s 50 Gb/s Ethernet and 100Gb/s Ethernet. Next to those there is IEEE 2.5Gb/s and 5Gb/s Ethernet. IEEE is continuing to work on standardizing higher bandwidths, such as 200Gb/s and higher.

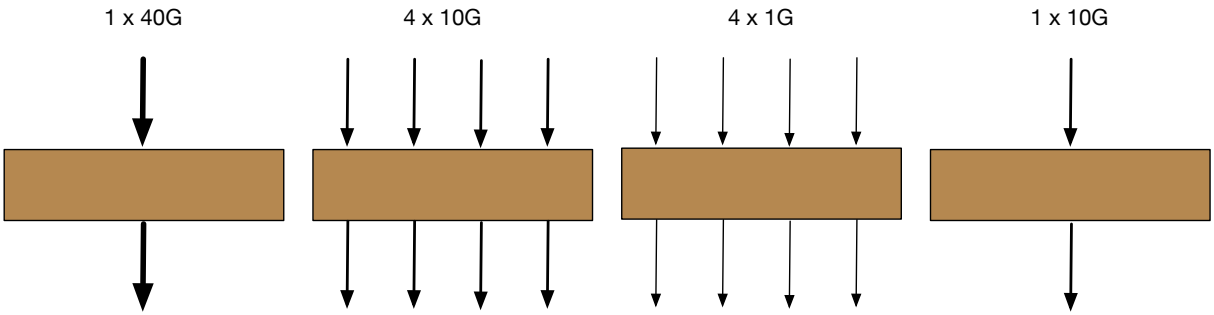
There are different options for network interfaces. Most of them are optical (SFP, SFP+, XFP, QSFP, QSFP+), with only RJ-45 being electrical.

https://en.wikipedia.org/wiki/Registered_jack
https://en.wikipedia.org/wiki/Small_form-factor_pluggable_transceiver
https://en.wikipedia.org/wiki/XFP_transceiver
https://en.wikipedia.org/wiki/QSFP

The bandwidth supported by an encryptor depends on the network interface and the software license. There is also the possibility of decoupling the encryptor bandwidth support from the bandwidths defined by the IEEE, as Metro and Carrier Ethernet support any bandwidth between 1 Mbit/sec and 100Gbit/sec. The processing power of the encryptor is defined by its overall implementation, not by the throughput of the network interface alone. The network interface just determines the maximum throughput.

In a Metro and Carrier Ethernet environment it can be beneficial to not have bandwidth support restricted to the IEEE standards. The support of incremental steps allows a customer to have a solution that scales with his needs and where he doesn't have to pay today for expected future needs. It is however obvious that e.g., a 10Gb/s encryptor limited by software down to 100Mb/s will cost more than a pure 100Mb/s encryptor. Encryptors that run close to 100% capacity will always attain the best price/performance ratio.

Some of the encryptors have multiple ports that – depending on vendor implementation – can be encrypted individually or combined.



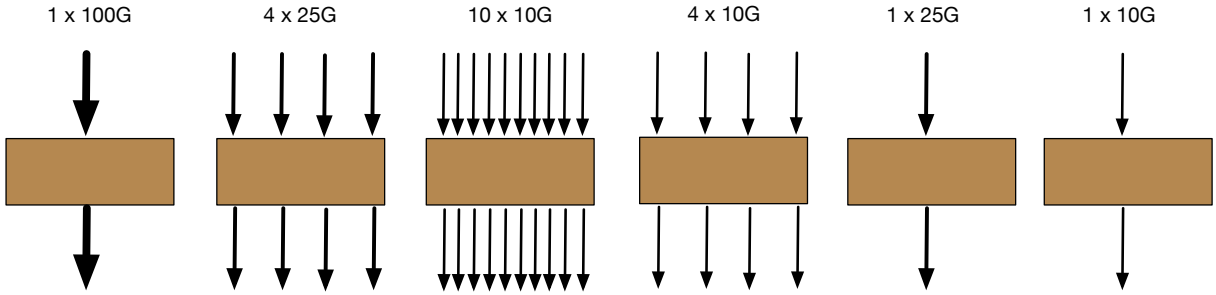
There is a significant difference between an encryptor designed for 1x40G and an encryptor designed for 4x10G: While single application has 40G available with a 1x40G encryptor, it only has 10G available with a 4x10G encryptor. The multi-port variant, on the other hand, has the advantage that ports can be used for different connections, depending on the overall architecture of the system.

- Different network segments

- Different network protocols and accesses (Ethernet, IP, Internet access), including for SDN scenarios
- Different customers
- One line per port secured with traffic flow security

The usage scenario and the applications decide, which is the more suitable solution: 1x40G or 4x10G. MACsec EDE is by definition a two-port bridge, which is why there are no multiport devices.

With a 100G encryptor, there are even more possibilities depending on the interface. In practice, only 1x100G is currently relevant:



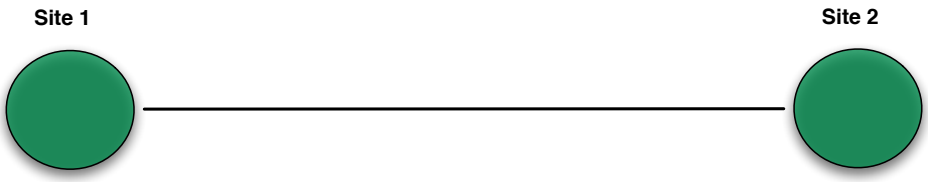
A limited number of vendors also offer their layer 2 encryptors as virtual appliances. Their security and performance depend on the operating environment. The characteristics of the hardware available to the virtual appliance are essential. Without dedicated and optimized hardware, not all crucial functions have direct hardware support anymore, despite still being available. This leads to a loss of security and performance. There are only a few cases, in which the use of a virtual layer 2 encryption appliance makes sense. Even then, there must be sufficient computing resources for the encryption. For random number generation/key generation and key storage there should be appropriate hardware available, such as a network-based HSM or a smart card. Theoretically it is even possible to secure a 100Gb/s connection with a virtual appliance, but only if the required computing resources are available. Such a setup will not meet the security level and the cost efficiency of a dedicated appliance, though.

2.2. Supported Network Topologies

Key system and available encryption modes are defining factors for the support of different network topologies and Metro and Carrier Ethernet standards.

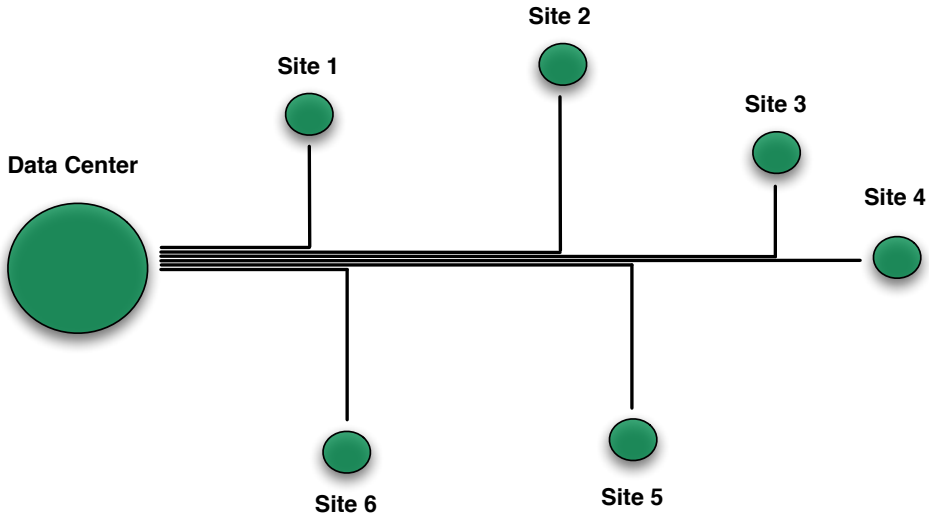
2.2.1. Point-to-Point

A point-to-point connection connects two sites.



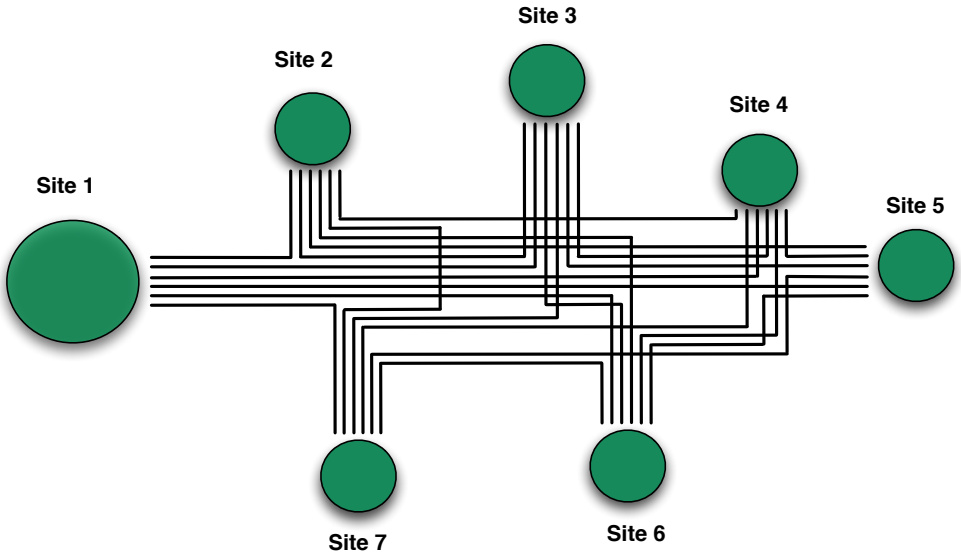
2.2.2. Point-to-Multipoint

Point-to-Multipoint topologies are multiple point-to-point connections or single point-to-multipoint connections that originate at the same central source.



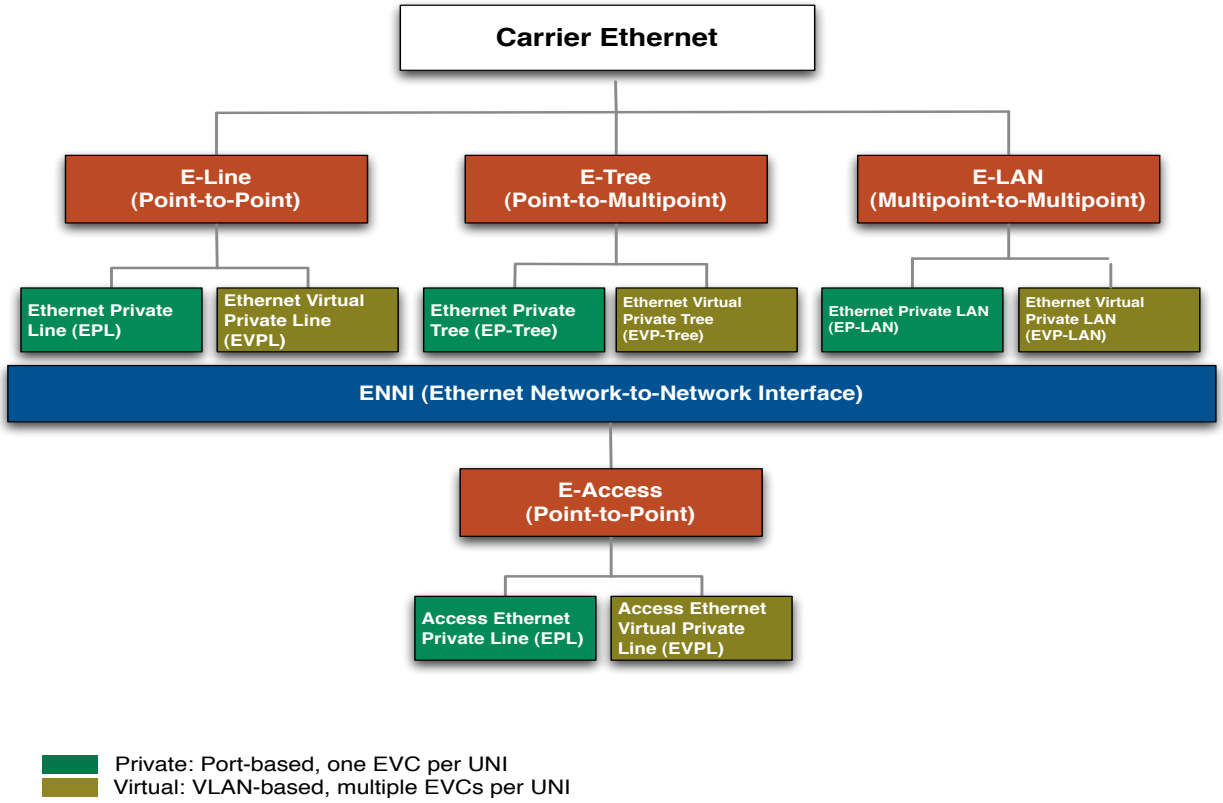
2.2.3. Multipoint-to-Multipoint

Contrary to a point-to-multipoint topology, a multipoint-to-multipoint topology supports the direct connection between all sites. There is no single central site. Each site in a multipoint-to-multipoint can communicate directly with all other sites in the network.



2.3. Supported Metro and Carrier Ethernet Topologies

Encryption mode and key management are decisive factors for the proper support of the different MEF topologies.



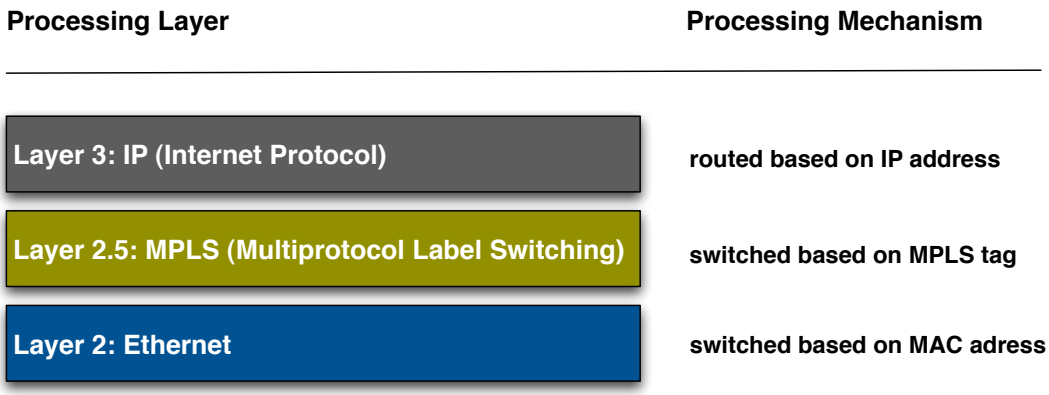
2.4. Networks Supported for Encryption

Carrier Ethernet can be viewed as layer 2 VPN, as network service for MPLS and IP networks and as access ramp to the public internet. Even as a combination of all of them.

Most of the products focus on Ethernet and layer 2 VPNs as each of the networks used for multi-site connectivity - Ethernet, MPLS and IP – has its own characteristics and requirements. Full support and security for MPLS- and IP-networks can only be accomplished with layer 3 encryption. There are a few offers on the market that support and protect all those networks natively for multisite connectivity from layer 2 up to layer 3.

MPLS networks mostly require delivery at layer 3 (IP). It is located at layer 2.5 of the OSI-stack and can be either secured at layer 2 (if MPLSoE is used) or at layer 3 (if MPLSoIP is used). MPLS networks switch packets based on MPLS tags. At every MPLS switch the Ethernet sender address of the incoming frame is replaced with the Ethernet address of the MPLS switch. A key system that is dependent on the sender address of the Ethernet frame thus will face unwanted issues. Encrypting IP at layer 3 requires that the encryptor provides complete support for layer 3 infrastructures for IPv4 and IPv6.

It is not common practice yet to secure mixed environments with a single encryptor yet. Often a different encryptor is used for layer 2 and layer 3.

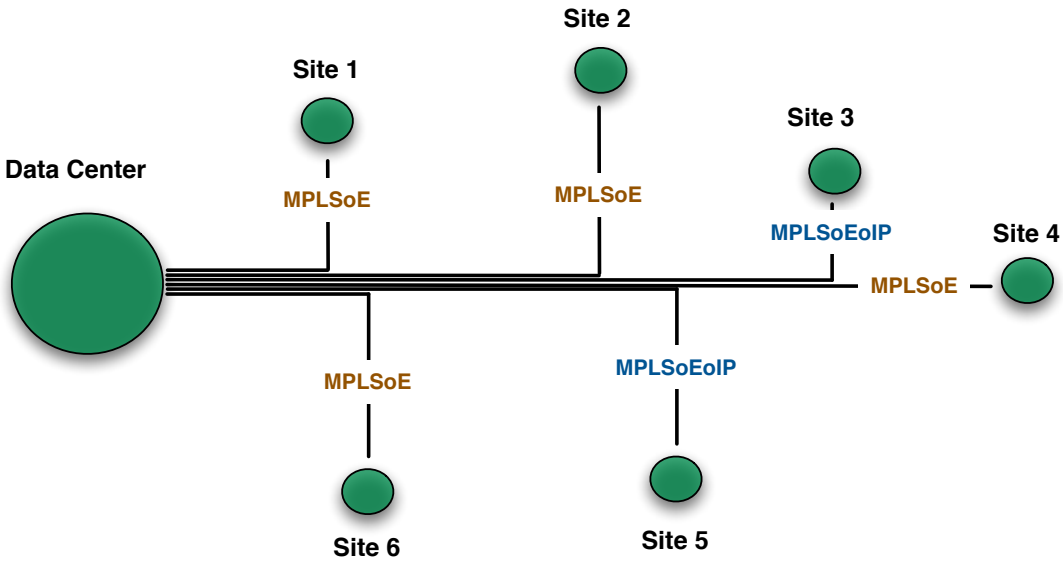


2.5. Networks Supported for the Transport of Encrypted Frames

There are scenarios for the transport of encrypted frames, in which transport networks other than Carrier Ethernet must be supported. In such cases an Ethernet encryptor limited to Ethernet does not fit the bill. On the other hand, there are encryptors marketed as Ethernet encryptors that are limited to encrypting Ethernet and transporting it over IP (EoIP). Such products make only sense in cases where no native Ethernet is available for the transport of Ethernet, as native encryption is much more efficient. Some native Ethernet encryptors offer EoIP as additional functionality without being limited to it.

It can also happen that MPLS is used as transport network for Carrier Ethernet. The encrypted frame is then transported over MPLS (EoMPLS). As the encrypted Ethernet frame becomes MPLS payload, a native Ethernet payload encryption will keep the frame transparent to MPLS.

It becomes much more complex, if the objective is to encrypt a MPLS network, where some of the sites are connected at layer 2 and some of the sites are connected at layer 3.

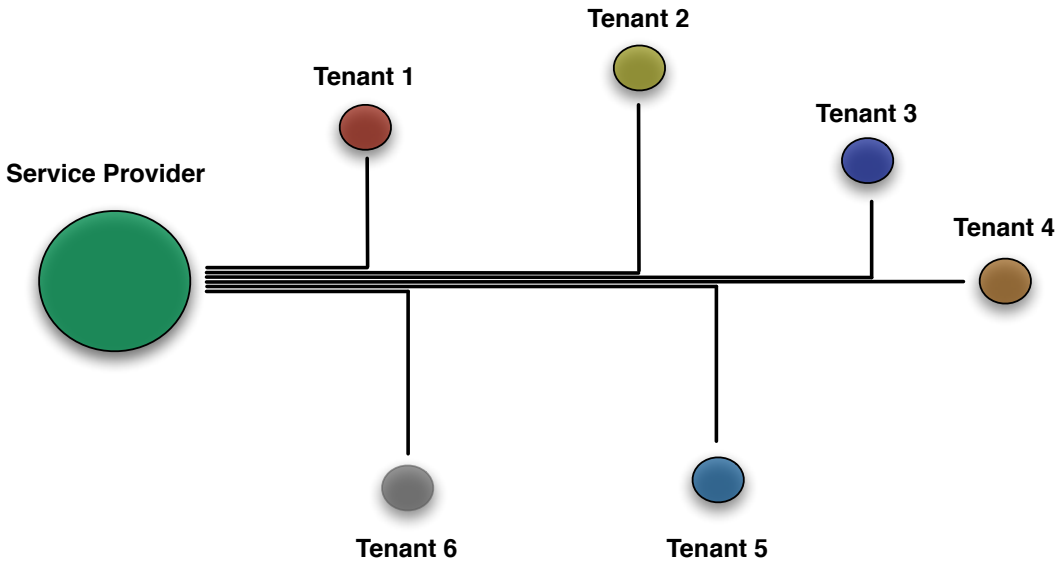


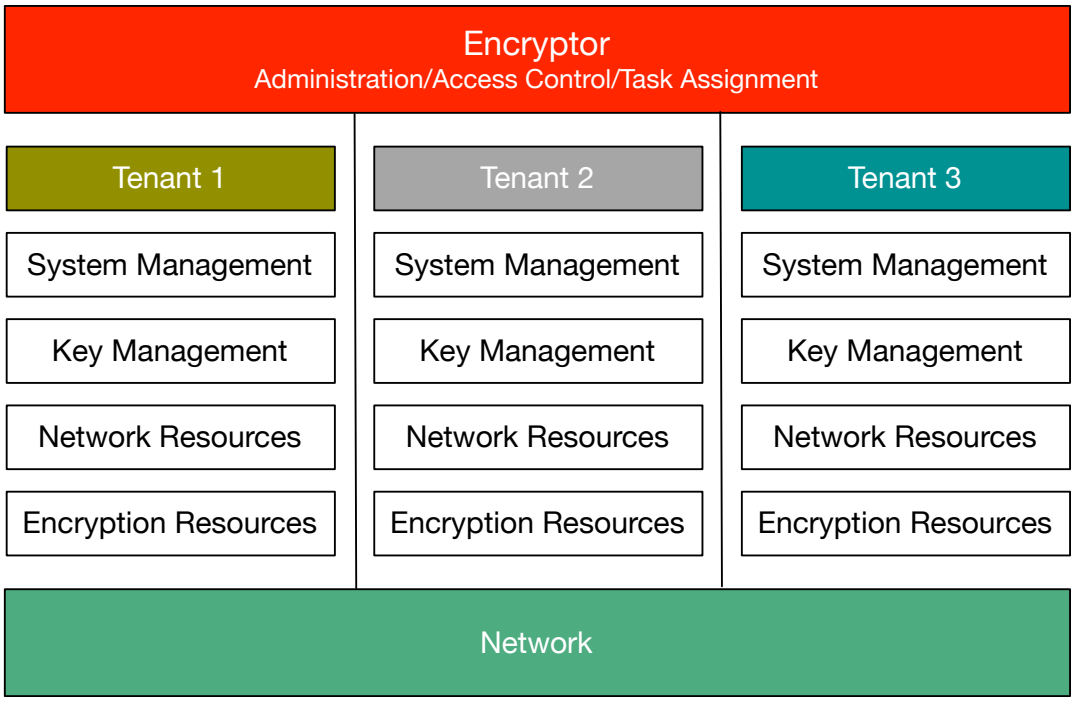
The demands in terms of encryptor functionality are substantially increased, as next to the frame transport over IP also key exchange over IP has to be supported.

Processing Layer	Processing Mechanism
Layer 3: IP (Internet Protocol)	routed based on IP address
Layer 2.5: MPLS (Multiprotocol Label Switching)	switched based on MPLS tag
Layer 2: Ethernet	switched based on MAC adress

2.6. Operating Scenario

Encryptors can be either self-managed or managed for a customer or tenant. For the latter the management software of the encryptor must support tenancy in order to enable Managed Encryption Services or Managed Security Services. A further scenario is the support of multiple different tenants. This requires multi-tenancy support by the management software and the key management system, includes two different authentication layers to be able to cryptographically separate groups/tenants.





If key ownership is to be with the tenant, additional requirements apply. When using certificate-based authentication and a different certificate authority per tenant there are particular challenges that need to be solved as it would be problematic to allow different CAs constant access to certificates located in an encryptor. The encryptors need the certificates for authentication and the certificates come from different root CAs, so that trust between the different CAs is a requirement.

This is much simpler if authentication takes place via pre-shared secrets. Each individual client can share one or more pre-shared secrets with the service provider and make future authentication impossible at any time by changing his pre-shared secret. However, care must be taken to ensure that pre-shared secrets are generated securely, stored securely, distributed securely, transported securely, and processed securely.

Different platforms use different approaches to tenancy and multi-tenancy. While some take an approach that requires a separate device per tenant, others take an approach that allows a different tenant to be assigned per port for multi-port devices. A third approach is to assign clients per VLAN or group. This allows multi-tenancy per port. A distinction must be made between multi-client capability per port or per multi-port device and the possibility of administering multiple clients with the same management system. In this case, the management solution is multi-tenant capable.

2.7. Platform Used

The number of vendors surpasses the number of the predominant platform developers. Only three of the vendors develop their own platform: Atmedia, Rohde & Schwarz and Senetas. All others use one of these three established platforms or follow IEEE 801.2AEcg.
IEEE 802.1AEcg is a MACSec-based platform that incorporated some input from the NSA Ethernet Security Specifications (ESS), but has neither found many supporting vendors nor many customers, except for the US government and the US administration. The other three platforms have been designed and optimized from start to meet the special requirements set

by Carrier Ethernet networks. Offers based on these platforms account for the majority of dedicated layer 2 encryption appliances sold and deployed worldwide. Not every product based on the same platform is necessarily identical. Some vendors do not limit the product differentiation to the front plate but others integrate additional code to differentiate the product and to meet certain certification requirements. In terms of certifications and approvals it has to be taken into consideration that a certification or an approval is not issued to a platform, only to products. Even if a platform developer receives certifications and approvals for his products, these are limited to his products. The products of vendors using that platform but selling it under their own name cannot profit from those certifications and approvals, even if the product is identical to the product of the platform developer.

The vendors that do not develop their own platform can be divided into two groups: The vendors that sell an existing product under their own name and the vendors that use a platform as base for their own product.

2.8 Operating Modes

Layer 2 encryptors should support different operating modes: Point-to-point (line mode) and multipoint (point-to-multipoint and mesh). These operating modes should be supported in all usage scenarios in a complete and autonomous way. As point-to-point is a subset of multipoint, each encryptor in multipoint mode can support point-to-point. This kind of point-to-point differs from what one would expect from a point-to-point encryptor that is optimized for point-to-point links.

For multipoint mode, the hardware requirements are drastically higher than for point-to-point as the complexity of the software (key management, key assignment, frame analysis, etc.) grows exponentially. Using such parameters such as VLAN-ID, MPLS tag, MAC address and QoS the encryptor has to process each single frame to and from each destination individually. The more destinations and options the higher the complexity and to keep everything secure. One of the bigger issues in that context is the key system as point-to-point encryption uses a pairwise key system, while multipoint encryption profits from group key systems.

3. Data Plane Encryption

3.1. Encryption Standard

All of the encryptors in this market overview that are supporting bandwidths up to multiple Gb/s use AES with a key length of 256 bit. Up to twelve years ago the most widely used block modes were Cipher-Block-Chaining (CBC) and the closely related Cipher-Feedback (CFB). In the meantime, state-of-the-art and the industry have moved to authenticated encryption (AEAD) and the de facto standard AES-GCM. GCM stands for Galois Counter Mode and combines authentication with integrity and replay protection. AES provides the confidentiality, whereas GCM provides authentication, integrity protection, replay protection, intrusion detection and intrusion prevention. In the context of layer 2 encryption it enables a layer 2 encryptor to serve as a layer 2 firewall.

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
http://en.wikipedia.org/wiki/GCM_mode

AES-CBC, which was predominant before the widespread use of AES-GCM, creates additional overhead by padding, unless used in combination with ciphertext stealing (CTS). As the implementation of CTS is rather complex, most developers do not make the extra effort.

http://en.wikipedia.org/wiki/Cipher_block_chaining
http://en.wikipedia.org/wiki/Ciphertext_stealing

The encryption block mode has a direct influence on the frame format, the frame overhead and the security. Current best security practice is the use AES-GCM. Today, enterprise-grade, government-grade and defense-grade encryption should use authenticated encryption (AEAD) with integrity and replay protection such as AES-GCM.

AES-GCM adds a frame overhead of 24-32 bytes, which is low compared to the security gained and to encryption with IPSec at Layer 3. The advantage comes from the fact that all IP traffic on Layer 2 can be encrypted and fully secured in transport mode at layer 2. While it is also possible to encrypt IP at Layer 3 in transport mode, the achievable security then falls short of that of tunnel mode because only the IP payload is encrypted. IP can be secured significantly more efficient on layer 2.

3.2. Encryption Hardware

There are different approaches to build an encryptor. The approach selected has a direct influence on the cost and performance. The vendors, whose products are capable of encrypting high-speed connections at full bandwidth independent of frame size all have a long experience and a hardware design that uses a high-performance FPGA. The increased development and production cost are compensated by the higher flexibility and performance. Not every FPGA is equal though, as performance and gate count differ between the diverse models and the encryption itself is just one of the jobs that is handled by the FPGA. A lower-cost, but much less flexible approach is the use of specialized security processors that come in the form of ASICs and take over the encryption function. Even lower cost is the use of software on a CPU, but that come at a price: Performance is dependent on the processing power of the CPU, the latency is increased and the security provided is lower.

3.3. Processing Method

Two different approaches exist for the processing of the frames, with each having its advantages and disadvantages.

An encryptor using the cut-through method starts with the encryption before the entire frame is read. This shortens the latency but results in the potential propagation of invalid frames, as invalid frames are not thrown away, but encrypted and sent to the target encryptor, which decrypts the first part of an invalid frame and passes it on to the next device, which then hopefully throws it away. Issues might also arise in case of missing data integrity when decrypting. If parts of the frame are transmitted before the integrity check took place, there is no way to pull them back. The next switch will have to throw those parts out.

The store-and-forward method reads the entire frame before starting the encryption or decryption process. This increases latency and makes the latency dependent on the frame size. Invalid frames can be detected and thrown away before the encryption process starts. Next to increasing the network hygiene the store-and-forward method also increases security.

3.4. Latency

The latency caused by the encryptor measures in microseconds per device. Decisive is the effective value per device and not just the latency caused by the actual encryption process. Product architecture and components used play an important role, with a latency of less than 10 microseconds offered by nearly every vendor of devices in the gigabit class. Factors responsible for varying latency on the same device are processing method, encryption mode and operating mode. Most of the vendors can supply the latency values for the different processing methods, encryption modes and operating modes in addition to the effective throughput values at given frame sizes and IMIX.

Latency should always be looked at in context with the overall latency of the connections as longer distance automatically leads to higher latency.

3.5. Encryption Offsets

The encryption offset is a feature that is highly relevant for network compatibility. It determines the starting point for the encryption and permits a full parameterization for the network that needs to be protected. Depending on the structure of the incoming frame and the desired limitation the encryption starts at a different location relative to the beginning of the frame. For a hop-by-hop encryption in a LAN it is sufficient to leave the MAC addresses unencrypted. In a MAN or WAN, the situation is different. The VLAN tag should be left unencrypted and if a MPLS tag is present, then that tag should be left unencrypted as well. In such an environment, the encryption should only start with the payload, independent of position of the payload within the frame. Feature-limited encryptors require the manual entry of a single, fixed encryption offset. Variable encryption offsets are much more flexible and can be a requirement in multipoint networks, especially if the incoming frames differ in terms of number of VLAN tags and MPLS tags. In those cases, it is preferable to have the encryptor being able to figure out where to start the encryption based on the frame content.

3.6. The Encryption Modes

The encryption modes supported by the encryptor determine which parts of the frame are encrypted. They are an important part of the key functionality of an encryptor.

- If the entire frame is encrypted, everything is efficient and secure, but limited to dedicated direct lines. No chance to profit from the lower cost offered by managed services.
- If the encryption covers only the payload, all protocols above layer 2 are completely secured, but the protection for layer 2 protocols is limited to the payload.
- If the entire layer 2 should be encrypted and the connection is over a shared infrastructure, the only choice is to tunnel the frames. This causes an overhead equal in size to the Ethernet header. This overhead can lead to frame sizes larger than supported by the network. Upstream traffic shapers in IPv4 networks can ensure that the frame size does not surpass the supported MTU. In IPv6 network packet size negotiation is handled between the communicating devices, which tend to be routers.

The encryption mode not only has an impact on the level of protection, but also on the operating cost, the latency and the hard- and software requirements. Encryption mode and encryption standard together define the frame format, which is the interface between encryptor and network and between the encrypted frame and the underlying network. Not all vendors support all encryption modes and there are important differences in the implementation of replay and integrity protection.

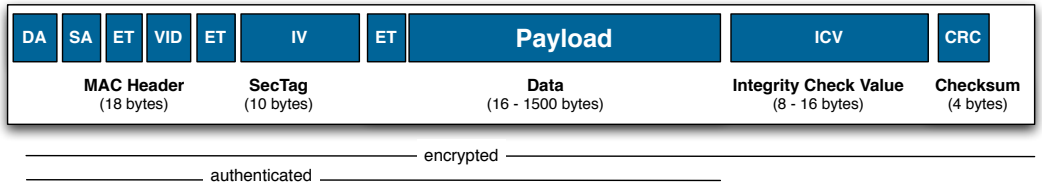
The encryption mode often has an impact on the scalability. A multipoint WAN can theoretically consist of thousands of sites, with the traffic between the sites handled by an encryptor at every site. In reality such large networks will be impossible to find, as a reasonable segmentation is the foundation for frictionless operation, efficiency and maximum security. While there are encryptors that could support an unlimited number of peers, in practice the support of up to 500 encryptors is amply sufficient. Actually, most broadband multipoint WANs consists of less than 100 peers.

The selection of the appropriate encryption mode is a question of finding the right balance between security, cost, network compatibility and overhead. The use auf unauthenticated encryption is not recommended.

The frame diagrams below distort the ratio between header/CRC and payload heavily to the disadvantage of the header and checksum.

3.6.1. Frame Mode

Bulk encryption encrypts the entire frame including Header and CRC checksum.



Frame Mode with Authenticated Encryption

Advantages:

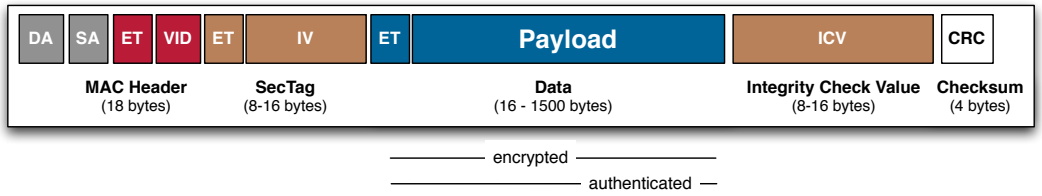
- All frames are completely encrypted
- Tapping the line will reveal nothing concerning network and data
- Authenticated encryption generates little overhead (24-32 bytes) compared to the security gained
- If unauthenticated, there is no encryption overhead on frame level

Disadvantages:

- Needs dedicated line
- Cannot be switched
- Has higher operating cost
- Incompatible with Managed Ethernet Services

3.6.2. Transport Mode

Transport mode limits the encryption to the payload, the header remains in clear. Most encryptors that support this mode permit to define the starting point of the encryption. Only the header information after the encryption offset will be encrypted, so that VLAN and MPLS tags can remain in the clear. This provides the necessary transparency of the frame for Carrier Ethernet and MPLS networks. Unless there is a dedicated line, the Ethertype field will also need to remain in the clear and remapped to avoid that the frame gets thrown out by interposed switches.



Transport Mode with Authenticated Encryption

Advantages:

- Entire layer 2 payload is encrypted
- Without explicit replay and integrity protection there is no frame overhead
- Frame-based replay and integrity protection have a excellent security/overhead ratio (only 24-32 bytes, depending on vendor)
- Can be switched
- Transparent to VLAN and MPLS (EoMPLS)
- Allows to procure bandwidth from the provider instead of leasing a dedicated line, leading to monthly cost savings of 30%+
- Compatible with Managed Ethernet Services

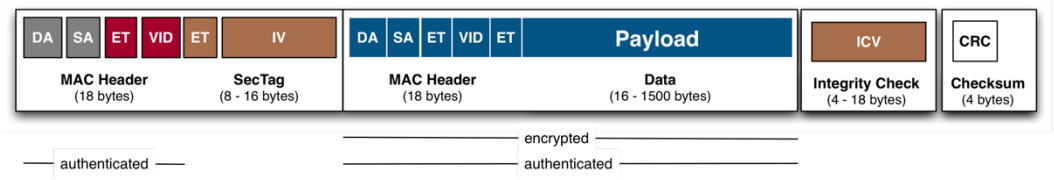
Disadvantages:

- Protection limited to layer 2 payload
- Tapping the line will reveal the LAN structure as the header remains in the clear
- Risk of MAC spoofing if the header or parts of it are not authenticated

3.6.3 Tunnel Mode

Tunnel mode encrypts the entire original frame while adding a new header and a new checksum. Sender respectively destination are the two encryptors on each side of the tunnel. The

newly created frame is a standard Ethernet frame that carries the original frame as payload. The tunneling generates an overhead of 18 bytes. Authentication adds another 24-26 bytes, bringing the total up to 42-44 bytes. This increases the latency by a couple of microseconds due to the additional processing required by the process. The overall impact on the network performance remains small.



Tunnel mode with Authenticated Encryption

Advantages:

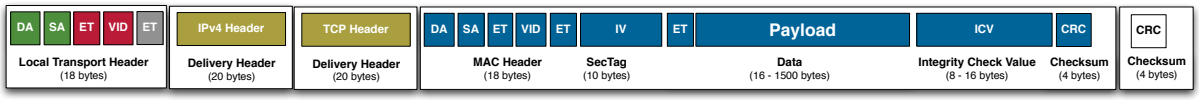
- Original frame is completely encrypted
- Can be switched
- Transparent to VLAN and MPLS
- Does not require dedicated line
- Compatible with Managed Ethernet Services

Disadvantages:

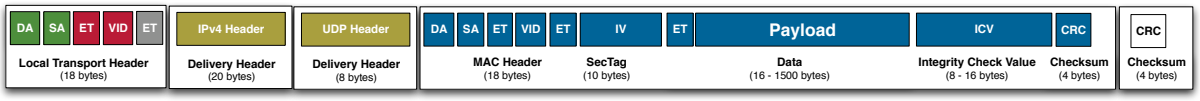
- Encryption overhead of up to 70% on frame level (with 64 byte frames), but averaging less than 10% in typical IMIX)
- Increases processing requirements
- Primarily optimized for point-to-point and point-to-multipoint
- Reduced scalability

3.7. IP-based Tunnel

It is also possible to transport Ethernet frames over IP, encapsulating an Ethernet frame as IP payload and encrypting the encapsulated Ethernet frame, or by encrypting the Ethernet frame and adding an IP header. If the entire payload is encrypted, then the protection of the payload is similar to that of a bulk encryption.



Ethernet over IP (EoIP) over TCP with authenticated encryption



Ethernet over IP (EoIP) over UDP with authenticated encryption

It is similar to an Ethernet tunnel, except that the encrypted original frame is not transported over native Ethernet, but over IP. In comparison with an Ethernet tunnel, an IP tunnel comes with more overhead and more latency. IP tunnels only make sense in environments where no layer 2 connections are available. If the transport of the encrypted frame is over IP, then also key exchange over IP must be supported.

3.8. Native IP Encryption for IP Networks

Native encryption of pure IP networks is also possible from Layer 2. As with Carrier Ethernet, the area of application is the encryption of static, broadband site networks. Key management is then based on the IP addresses, not the Ethernet addresses. Layer 2 encryptors operate in bridge mode for IP encryption as well.

IP encryption with Layer 2 encryptors is primarily an alternative to GETVPN and GroupVPN. The latter use IPsec ESP tunnel mode in combination with GDOI (Group Domain of Interpretation).

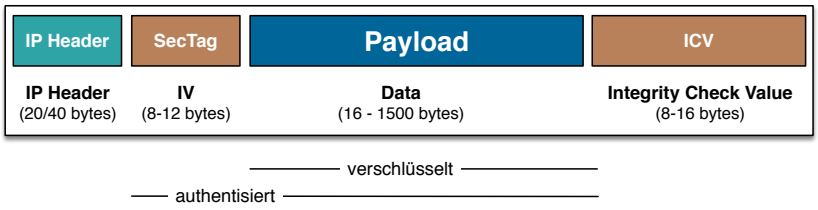
https://en.wikipedia.org/wiki/Group_Domain_of_Interpretation

IPsec between gateways is usually operated in ESP tunnel mode. For the outer header, the gateway addresses are used, while the entire original packet including the original header is transported and encrypted as payload. This is different with GDOI. An intermediate form between transport mode and tunnel mode is used, the transport tunnel. In this mode, the original header or the essential parts of it are copied into a new transport while the entire original packet including the original header is carried and encrypted as a payload. The internal addresses remain visible. Both Cisco's GETVPN and GroupVPN use this in the context of IPsec. The terminology used, varies by vendor. For GETVPN and GroupVPN it is a tunnel-less tunnel with "header preservation". Not all encryption solutions with group keys blindly take over all parts of the original header, though. Therefore, the term "header preservation" does not apply to all solutions. Transport Tunnel is more appropriate as a generic term. The typical application area for group key systems for IP are MPLS and virtual private IP networks.

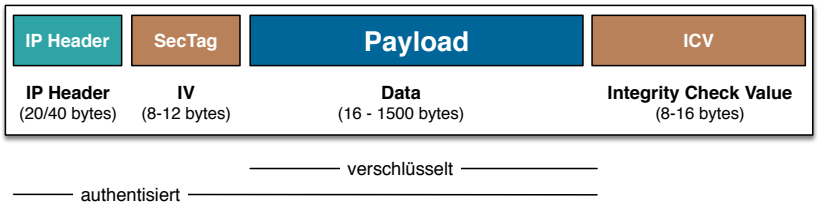
For use over public networks, the address separation of internal and external network can be outsourced to the router by means of tunnels. If the IP packets are already tunneled by the router (IP-over-IP), the encryption of the entire original IP packet can then be performed by the encryptor in transport mode, since the original IP packet arrives at the encryptor as an IP payload. However, the packet overhead generated by the IP-over-IP tunnels (20-40 bytes) should then be included in the calculation of the encryption overhead.

Group key management for IKEv2 is not yet standardized, only for IKEv1. Layer 2 encryptors use neither IKE nor IPsec for IP encryption.

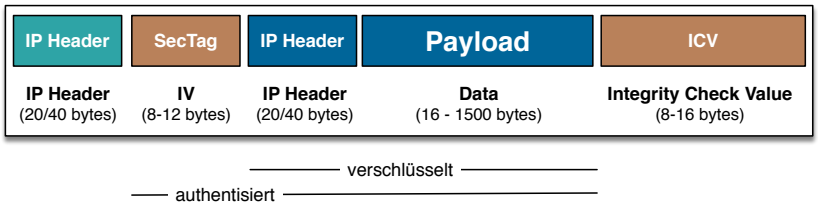
Below are the different packet format and encryption options:



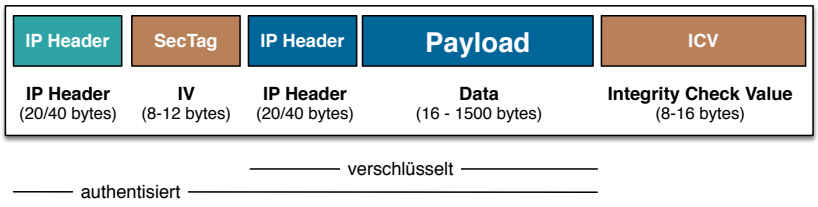
Transport Mode without Header Authentication



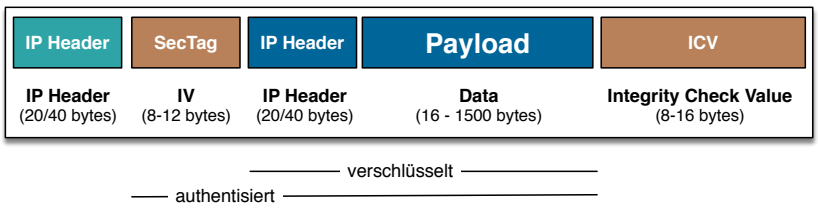
Transport Mode with Header Authentication



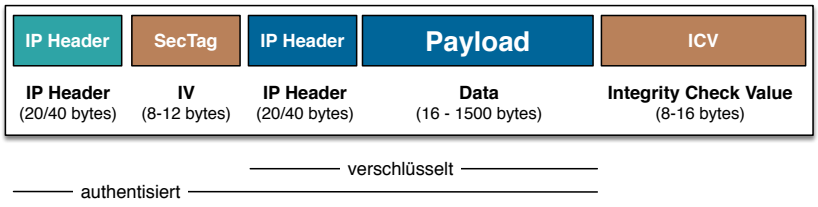
Transport Tunnel Mode without Header Authentication



Transport Tunnel Mode with Header Authentication



Tunnel Mode without Header Authentication



Tunnel Mode with Header Authentication

Compared to IPSec/GDOI-based solutions, the encryption overhead is often lower. Accordingly, Layer 2 encryptors with native IP support are mainly used in MPLS and IP networks where a reliable and powerful alternative to GETVPN or GroupVPN is required. Some of the encryptors can encrypt both Carrier Ethernet and IP in parallel.

3.9. Size of the Replay Window

Authenticated encryption with AES-GCM uses a counter. The sending encryptor increases the counter reading by one for every authenticated frame he sends. At the receiving encryptor the counter reading for each incoming authenticated frame from the sending encryptor should increase by one as well. Especially in MANs and WANs it can happen, that the proper sequence is not maintained. Depending on the network quality thus a window is required, that determines, how much deviation from the standard sequence will be accepted. This window has to be small enough to still prevent replay attacks. The replay window can be either defined by the maximum permitted deviation of the counter reading or by time in seconds.

3.10. Selective Encryption

There are scenarios in which frames with specific characteristics should or must be treated differently than the norm. That can be e.g., frames of a VLAN that is used to provide the outside connection to the Internet or frames with an MPLS tag. All information contained in a frame can be used as criteria: VLAN-ID, MPLS tag, Ethertype, MAC address and IP address. It is also possible to use factors such as CoS/QoS or frame size. Selective encryption is a functionality that allows addresses and connections to be treated differently including exclusion from encryption. Key selection criteria are MAC address and VLAN ID. Many Carrier Ethernet services are based on VLAN IDs and selective encryption by VLAN ID is required for certain services. This feature allows using a single access line for multiple services, such as Ethernet, MPLS and Internet. Such a consolidation of access lines can offer substantial cost savings. “MPLS awareness” combined with selective encryption based on the presence of an MPLS tag is required to master different MPLS scenarios.

3.11. Extended Security Functions

For deployments with increased security requirements, the different platforms provide additional security functions.

3.11.1 Modifiable S-box

In cryptography, an S-box (substitution box) is a basic component of a symmetric key algorithm that performs a substitution. In block ciphers, they are commonly used to modify the relationship between the key and the ciphertext. The modifiability of the AES S-box is a standard functionality of AES. The standard parameterization of the S-box can be replaced in the AES encryption scheme with a custom one. This ensures that it will not be sufficient to have the key and a standard AES decryption to decrypt the ciphertext. It is also a mean to exclude a backdoor built into the encryption algorithm that exploits a static S-box.

3.11.2 Traffic Flow Security

Traffic flow security can be used to obfuscate network traffic by modifying the actual traffic flow transported over the network. There are different approaches: (1) Simple padding by adding bytes of additional data to frames to slightly obfuscate actual frame sizes, (2) uniform frame sizes with additional padding, and (3) injection of synthetic network traffic to fill up the available bandwidth. Only the injection of synthetic network traffic can do a perfect job. The other approaches come with limited benefits in terms of obfuscation, with increased latency and jitter, and most often also with a reduction of the IMIX throughput. TFS implementations use tunnel mode for encryption.

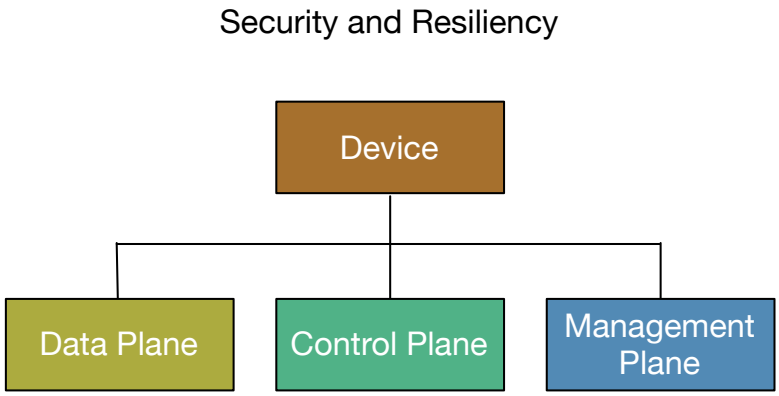
Implementations based on fixed MTU sizes work in tunnel mode. Frames are split or combined to match the fixed size of the MTU. If a large MTU is selected, then multiple frames might have to be combined in order to match the MTU size. This adds latency and jitter. The alternative is to use padding for reaching the desired MTU size for smaller frames. This adds jitter. If a small MTU size is selected, then large frames need to be fragmented into multiple frames. This adds latency and jitter and increases encryption overhead.

At this time, only two platforms offer traffic flow security, only one of them offering synthetic traffic injection. In its next revision, due in 2024, MACsec EDE will support tunnel mode and

traffic flow security. It is however based on fixed MTU size and thus way behind the state-of-the-art available on the market since more than 10 years.

4. Control Plane Protection

Metropolitan Area (MAN) and Wide Area Network (WAN) security is deployed at the edge of each site. A viable solution must provide network security and resiliency. This requires overall security and resilience, encompassing device, data plane, control plane and management plane. It is not sufficient to protect the data plane as good as possible. Encryption needs key and those keys must be exchanged between the devices. The key exchange is therefore as popular a target for an attack as the device itself, the management plane and the rest of the control plane.

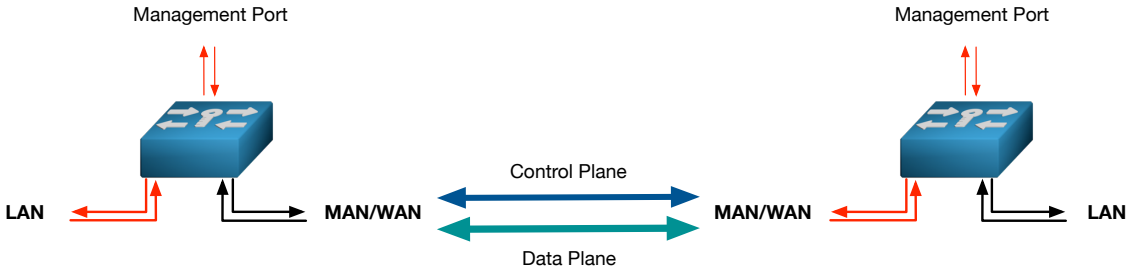


A single weakness in one of those four areas will compromise security and resiliency. A secure device is the foundation. Dedicated network encryption appliances can provide the required level of security and resilience.

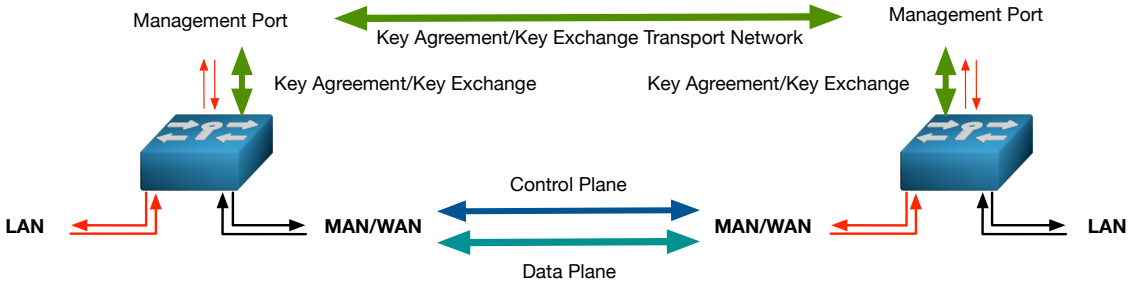
4.1. Configuration Options for the Control Plane

The control plane can either be transported together with the data plane over a MAN or a WAN, or it can be transported over another secure network, using that network's security for protection. The control plane is not limited to key exchange, but also carries control and status messages.

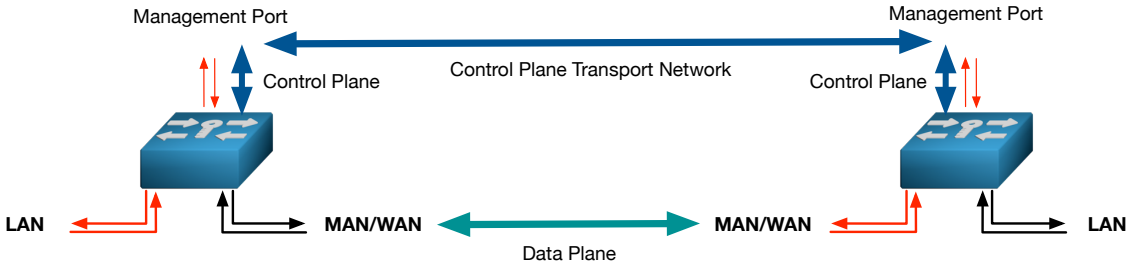
There are different configuration options for control plane and key exchange. Most often, control plane and data plane are transported in-band over the same network, with the key exchange taking place over the control plane.



Another configuration option is to separate the key exchange from the control plane and transport it via management port over another secure network.

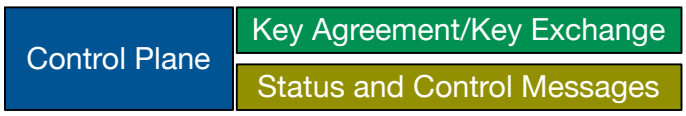


Another configuration option is to transport the entire control plane via management port over another secure network.



4.2. Securing the Control Plane, Key Agreement and Key Exchange

If the control plane is transported over the same network as the data plane, the same threat scenario applies for the control plane as for the data plane.



Control plane data and control plane network must be properly protected.

The most secure approach is to protect the control plane including key agreement and key exchange equivalent to the data plane using authenticated encryption at the network layer, using the same hardware support as the data plane encryption does. Using an FPGA increases the resilience against denial-of-service attacks compared to the use of a CPU.

The protection of the control plane, the key agreement and the key exchange at network level is an area that has been mostly neglected until recently.
The problem of securing the control plane, key agreement and key exchange at the network level is an area that has received too little attention in the past. In the meantime, the IEEE has also admitted the weaknesses of MACsec in this area. On page 34 of the current standard the following can be found: „Page 34:

MACsec does not protect against brute force denial of service attacks that can be mounted by abusing the operation of particular media access control methods through degrading the communication channel or transmitting erroneous media access method specific control frames ".

Some vendors of specialized appliances that do not use MACsec, do protect the control plane as well as the data plane, treating the communication between the devices as a network that has its own network encryption.

5. Auto-Discovery and Key Server

5.1. Auto-Discovery

Auto-discovery simplifies the initial configuration of the encryptors and the adaption to configuration changes. It allows an encryptor not only to see the other encryptors in the network, but also to detect key servers and VLANs. Once the encryptors are configured, it must be possible to disable auto-discovery and lock the configuration. It will only be needed again in case of network configuration changes.

5.2. Key Server

Every device that generates and distributes keys to other devices is a key server. There are different ways to implement key generation and key distribution. In case of a symmetric key system, it is even possible to generate and distribute only the information necessary to calculate the key instead of the key itself.

5.3. Integrated Key Server

Encryptors with integrated key server do not require an additional external key server. Depending on the usage scenario and on compliance and on regulations, the additional use of an external key server can be beneficial or might even be a requirement.

5.4. Support for External Key Server

Depending on the usage scenario, regulations and company policies, using an external key server can be advantageous or even a requirement. External key servers can be either used to separate key management and encryption, to enhance security or to improve scalability. The separation of key management and encryption is often used in a managed encryption services scenario, in which the customers want to retain physical ownership and access to the key server, next to owning the keys.
Integrated and external key servers do not exclude each other mutually. In large networks, it can be advantageous to use a combination of integrated and external key servers. Depending on the number of master keys in use and the frequency of their change an external key server can be beneficial for the scalability. An external key server is subject to the same security requirements as an encryptor.

In the case of certificate-based asymmetric encryption an external Hardware Security Module (HSM) can serve as Certificate Authority (CA). A HSM can also be used as external key server or for key generation and key storage for virtual appliances.

Another scenario is the combination of encryptors with quantum key distribution, where the keys are generated and distributed over a separate line.

5.5. External Key Server

Only a couple of vendors offer external key servers. They are normally used in large networks, managed encryption services and high-security environments and come in the form of network-attached key servers, HSMs, and QKD-devices.

5.6. Support for Multiple, Distributed Key Servers

A single key server can fail and thus constitutes a single point-of-failure (SOF). Another issue is the dependency on uninterrupted availability of the connection to the encryptors to the key server. Multiple, distributed key servers allow the encryptors to maintain secure operation even if a key server fails or a connection is interrupted. For multi-tenancy scenarios with key ownership by the tenants, multiple, distributed key servers are a requirement.

5.7. Support for Fail-over to Backup Key Server

In group key systems in which all group members use the same key to encrypt and decrypt frames, a group key server supplying such a shared key to all group members is required. If such a group key server fails or becomes unreachable, no further key exchange and group membership check is possible. To avoid such a scenario, group key systems normally have a hierarchy of multiple, distributed key servers. If the currently active group key server fails or becomes unreachable, the next in the hierarchy takes over.

In the case of group key systems, in which an encryptor with integrated key server only distributes the keys to decrypt the keys for frames sent by him, there is no need for a backup key server. If the encryptor fails or becomes unreachable he cannot send frames anymore and no keys are required to decrypt frames that are not sent.

6. Key Management

Key management is the core of every network encryption solution. It is to a large degree responsible for determining the application area and the functionality.

6.1. Basic Foundation

Truly random random numbers, secure key storage and autonomous operation are part of the basic equipment needed for a solution that wants to secure networks between sites. Virtual appliances can only accomplish this with the help of additional hardware, such as smartcard.

6.1.1. Hardware Random Number Generator

Secure cryptographic solutions are dependent on the availability of truly random random numbers. Software can only generate pseudo-random random numbers, but no true random numbers. Secure solutions use a hardware random number generator to generate the random numbers needed for key generation.

http://en.wikipedia.org/wiki/Hardware_random_number_generator

6.1.2. Secure Key Storage

Keys need to be protected from unauthorized access, as the security of the system is dependent on the security of the keys. Thus, keys and initial secrets, such as shared secrets, the private key of the certificate, etc. must be stored in a secure fashion. So secure that any attempt to manipulate lead to an immediate zeroization of the entire content of the storage. The key storage must be tamper resistant.

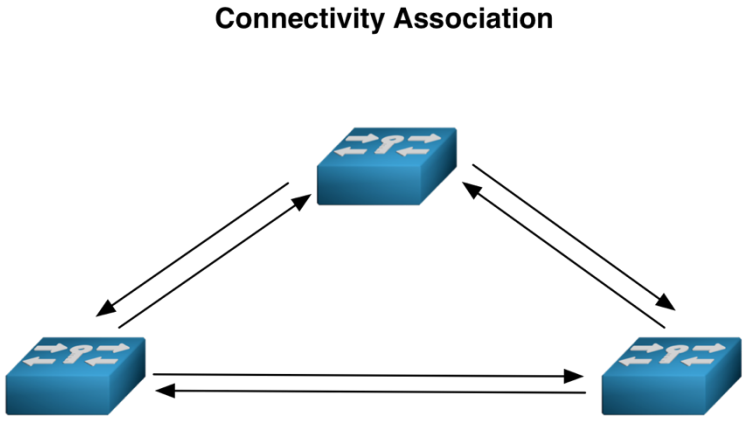
http://en.wikipedia.org/wiki/Tamper_resistant

6.1.3. Autonomous Operation

Autonomous operation requires that the encryptor accomplish its job independently of external resources. Each external resource constitutes a risk and a dependency. Dedicated key servers, certificate authorities and dedicated security management are not considered to be external resources. Such devices should not be single points of failure, though and should be configurable in a redundant fashion.

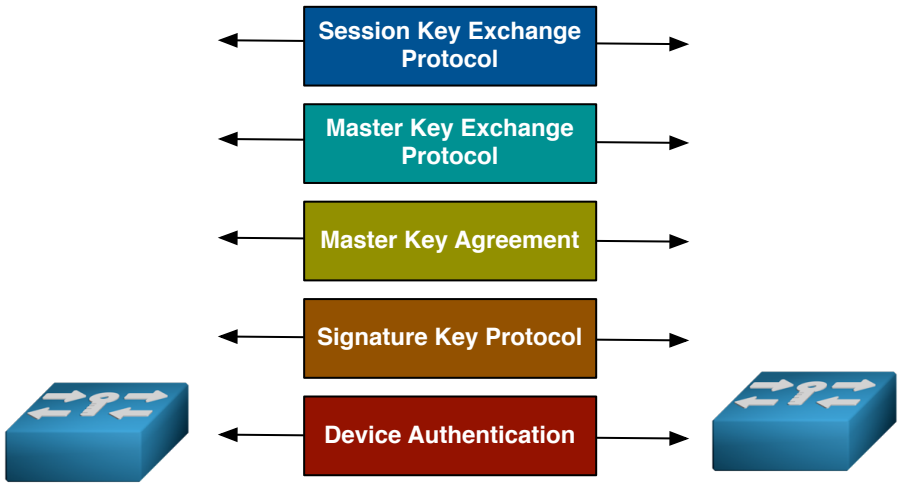
6.2. Connectivity Association

Communication involves more than a single party. All participating encryptors must find each other, recognize each other and authenticate themselves mutually. Once that is accomplished there is a connectivity association between each of the participating encryptors. They are authorized to communicate with each other.



Once the connectivity association is established, a security association can be built, that determines how the two participating encryptors are communicating securely. This is accomplished using an initial secret and a key agreement protocol. The initial secret can be a pre-shared key or a certificate. In case of elliptic curve cryptography, the curve domain is also an initial secret that needs to be present. The initial secrets are stored in a secure key storage.

In the build-up from initial secret to session key multiple complex processes take place. Each of them needs to be secure by itself and in the sequence, it is being used.



Most encryptors use a hybrid approach, employing a combination of asymmetric and symmetric encryption. For the data traffic, symmetric encryption is used.

6.3. Authentication/Initial Secret and Signature Protocol

The encryptors must authenticate themselves to one another. This can be done either by certificates (asymmetrical) or by using pre-shared secrets (symmetrical).

http://en.wikipedia.org/wiki/Shared_secret
http://en.wikipedia.org/wiki/X.509

Authentication using pre-shared secrets can be done between a pair of encryptors, between all members of a network, per group or per pair of encryptors in a group.

The initial secretes, pre-shared secret or certificate, are used for signing in order to allow the recipient to verify the sender. The key exchange uses them to sign the keys or partial keys that are exchanged to ensure that they are coming from the correct remote device.

http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/RSA
http://crypto.stackexchange.com/questions/14654/digital-signature-using-symmetric-key-cryptography

The signature in combination with the signature protocol is the foundation for the key exchange.

6.4. Key Exchange

There are two different approaches to key exchange: One is symmetrical and the other one is asymmetrical. The asymmetrical approach needs more computing power but is considered to be more secure. Some physicists, technologists and mathematicians are assuming that a quantum computer with the proper algorithms could solve the mathematical problems used as foundation for asymmetrical key exchange within minutes and that powerful quantum computers might become a reality within the next decade. A big jump in security that also prevents successful attacks by quantum computers is therefore provided by a combination of asymmetrical and symmetrical key exchange, such as the combination of Diffie-Hellman with symmetrical encryption of the partial keys. A 256 bit AES key is used as signature and makes the key exchange immune against attacks from quantum computers.

6.4.1. Symmetrical Key Exchange

In a symmetrical approach, all keys are directly derived from each other. First, a shared secret is entered into the encryptor. Then the encryptor generates internally a master key and encrypts the master key with the shared secret. The session key is also generated by the encryptor and is encrypted with the master key. Master key and session key are transmitted to the other encryptor in encrypted form. The big issue with this approach is the shared secret. If that shared secret ever becomes known, then all previously recorded data communication can be decrypted.

http://en.wikipedia.org/wiki/Symmetric_key_algorithm
http://en.wikipedia.org/wiki/Symmetric_key_management

6.4.2. Asymmetrical Key Exchange

In an asymmetric approach the partial keys are generated completely inside the encryptor, without any user having access to it. After exchanging the partial keys both sides calculate the same shared secret. Contrary to a symmetric approach, nobody knows the shared secret. Subsequently the encryptor generates internally the master key and encrypts it with the shared secret. The encryptor also generates the session key and uses the master key to en-

crypt it. The transmission of the master and session keys from one encryptor is always encrypted.

Common asymmetrical approaches are Diffie-Hellman and RSA. Diffie-Hellmann uses in its basic variant the discrete logarithm problem, which comes with the disadvantage of needing very long partial keys to be really secure. The same is true for RSA. A more state-of-the-art variant is the use of Diffie-Hellman with elliptic curve cryptography (ECC), which provides better security with shorter partial keys. The security of ECC is heavily dependent on the curves used. Some vendors give users the choice between NIST curves, Brainpool curves, Safecurves and custom curves, while other support NIST curves only. The generation of secure elliptic curves is complex and the proper implementation of elliptic curve cryptography is non-trivial as well. There are also speed differences between the different elliptic curves, but for multisite networks they do not really matter.

http://en.wikipedia.org/wiki/Diffie-Hellman
http://en.wikipedia.org/wiki/RSA
http://en.wikipedia.org/wiki/Elliptic_Curve_Diffie-Hellman
http://safecurves.cr.yp.to/index.html
http://www.ecc-brainpool.org/links.htm
https://tls.mbed.org/kb/cryptography/elliptic-curve-performance-nist-vs-brainpool

Asymmetrical approaches sign the partial keys that are exchanged to ensure that the correct remote station sends them. There are different ways to accomplish this: Either by using a certificate (X.509) in combination with appropriate procedures (RSA, DSA or ECC) or by encrypting the partial keys with a pre-shared secret.

Most systems use a hybrid approach. Session keys are always symmetric.

6.4.3. Quantum-safe Key Exchange

The threat by future quantum computers is limited to the asymmetrical key exchange, as long as the symmetrical encryption uses 256-bit keys. There are different approaches to mitigate the risk relating to the asymmetrical key exchange today:

- Symmetric key exchange
- Asymmetric key exchange with additional symmetric pre-shared symmetric key as element
- Symmetric encryption of the asymmetric key exchange
- PQC (post-quantum cryptography)
- QKD (quantum key distribution)

https://www.ipspace.net/kb/QuantumCrypto/
https://www.uebermeister.com/en/networksecurity/quantum-safe

Some vendors offer some of the options listed above. In terms of PQC, there is no definitive standard yet.

6.4.4. Exchange Frequency

The more frequent the sessions keys in use are replaced, the lower the probability that the key will be compromised. The security of the key does not only depend on the secrecy of the key, but also depends on the process used and the parameters chosen. The length of the counter and the ICV play an important role. E.g., in counter mode the key has to be changed

before the counter starts back at 0. With group key systems is therefore required that the system automatically changes the session key after a given number of minutes.
The same is true for the key encryption key (master key), which is used to encrypt the session keys. The exchange frequency is lower as it is only used to encrypt the session key and thus is used less often and encrypts less data. The regular exchange of master keys should take place automatically after a certain period of time. Key exchanges using Diffie-Hellmann are compute-intensive. Sufficient processing power of the encryptor is a requirement for keeping the lifecycle of a master key low, especially in large, complex networks.

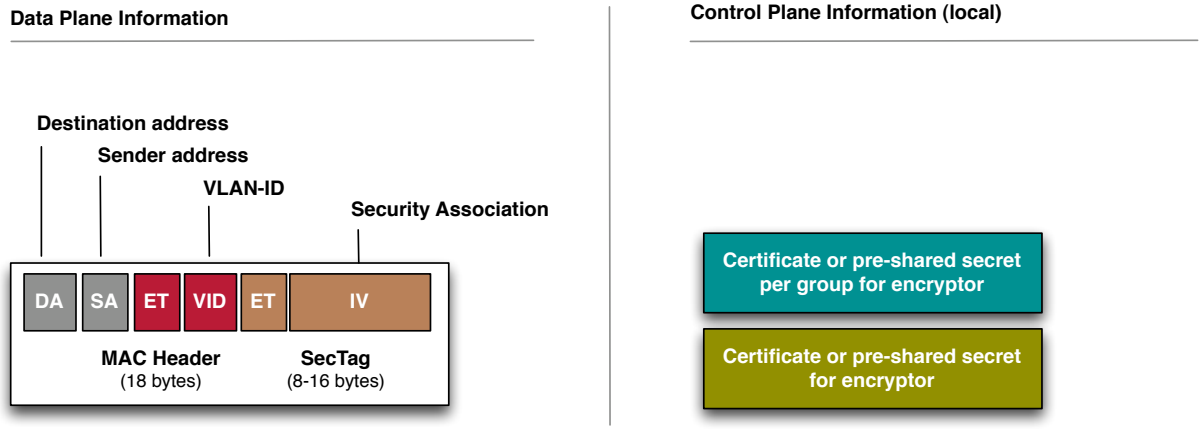
Key Type	Change Frequency
Session Key (Data Encryption Key)	every 1 - 60 minutes
Master Key (Key Encryption Key)	every 1 -24 hours
Initial Secret	every 12 - 24 months

6.5. Key System

Ethernet frames come in three different variants, depending on the number of recipients of a frame:

Unicast for the communication of one MAC address with a single other MAC address
Multicast for the communication of one single MAC address with multiple MAC addresses
Broadcast for the communication of one single MAC address with all other MAC addresses

There are different approaches to ensure that next to unicast frames also multicast and broadcast frames are properly encrypted. The foundation for the key system is established on one hand by the initial secrets located in each encryptor and on the other hand by the information carried by each frame.



There are two different approaches for key systems: Pairwise keys and group keys.

For pairwise key system a network consists of a multitude of point-to-point connections. Each encryptor is connected with each other encryptor by a point-to-point connection. Traditional pairwise key systems use unidirectional keys for the connection between a pair of encryptors.

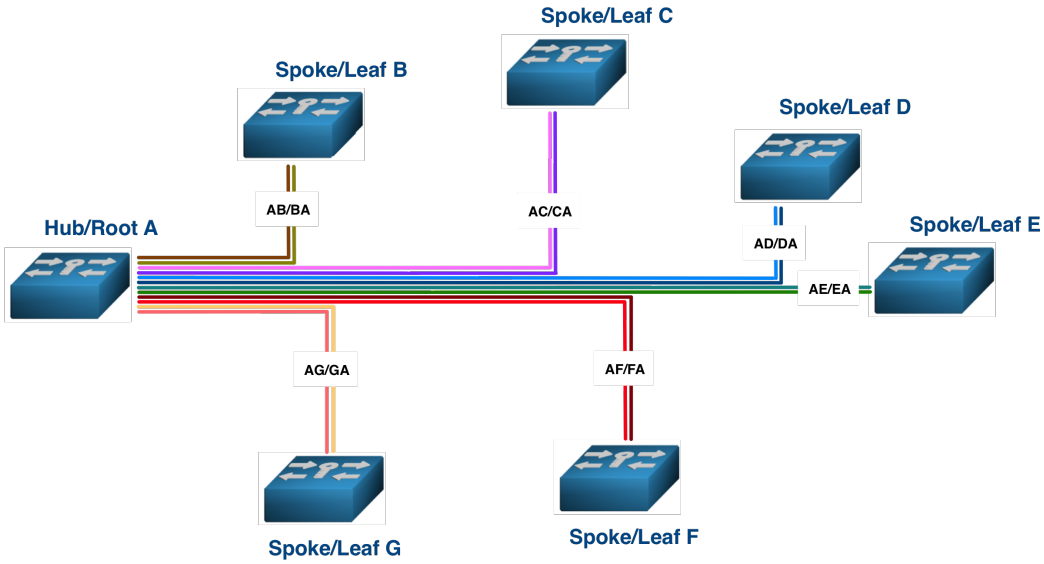
Group key systems are based on group membership and use a different key per group. There are different ways to define a group. A group can e.g., consist of a VLAN or multiple VLANs. In such a definition, the group is bidirectional. Each group member uses the same key to encrypt and decrypt frames. A group can also be defined to consist of the recipients of a sender's frames. In such a definition, the group is unidirectional. Each encryptor uses a different key to encrypt frames and the recipient uses the key provided by the sender to decrypt the frames coming from that sender. An encryptor can support multiple groups. For each of those groups he uses a different key and in the case of unidirectional groups he uses as many keys as there are members in the group.

Further it is possible to use a combination of a pairwise and a group key system. From an organizational point of view a VLAN can constitute a group, in which pairwise keys are used for unicast traffic and a group key is used for multicast and broadcast traffic. For each VLAN separate pairwise keys and a separate group key are used.

6.5.1. Pairwise Keys

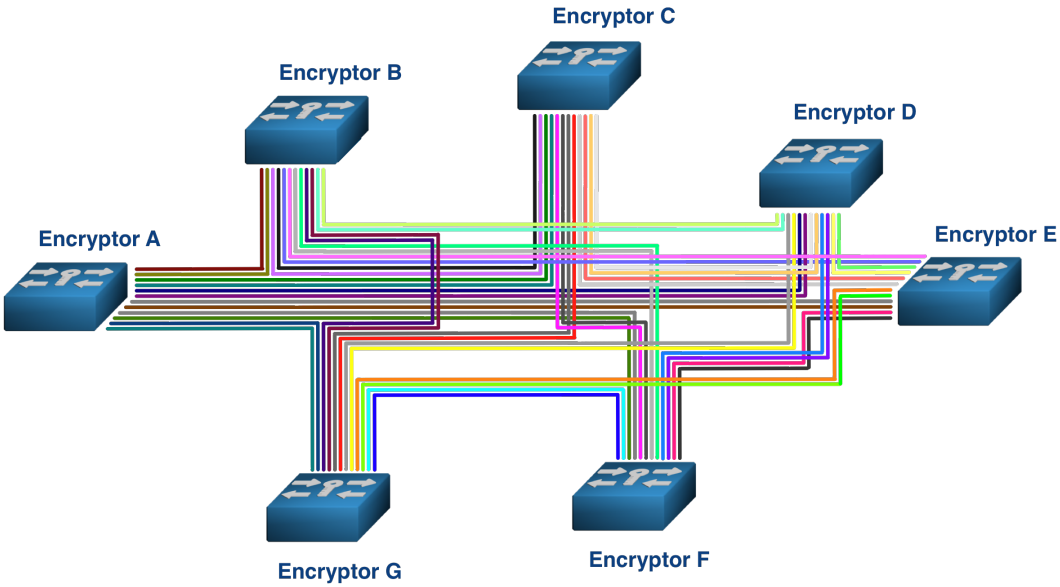
For a pairwise key system point-to-point connections consist of a link whose end-points are defined by the two encryptors A and B. For the encryption of the data flowing from A to B the encryptor uses key AB. In the opposite direction, from B to A, the encryptor uses key BA.

Pairwise keys systems are designed for point-to-point connections and therefore also treat point-to-multipoint and multipoint networks as an accumulation of point-to-point connections.



Pairwise key systems are designed for point-to-point connections and function only with unicast frames, as unicast frames are limited to a single destination, unless a point-to-multipoint topology is set up as an accumulation of separate point-to-point links with individual multicast and broadcast frames. Multicast and broadcast frames have a single sender, but multiple destination addresses. This spells trouble for pairwise key systems as there are no pairwise keys for a frame with multiple destinations. By definition a pair is limited to two and that means that there can only be a single destination. E.g., there is no key available for encryptor A to encrypt a multicast frame for two different destination encryptors (B and C) and that would also be available for the destination encryptors to decrypt the frame.

Pairwise key systems also treat multipoint-to-multipoint topologies the same way they treat point-to-point connections.



There are four different solution approaches for this problem: (1) Leave multicast and broadcast frames unencrypted, (2) replicate multicast and broadcast frames for every connection and then treat them as unicast frames, (3) add a specialized key system take care of multicast and broadcast frames, and (4) use a key system that can handle unicast, multicast and broadcast frames.

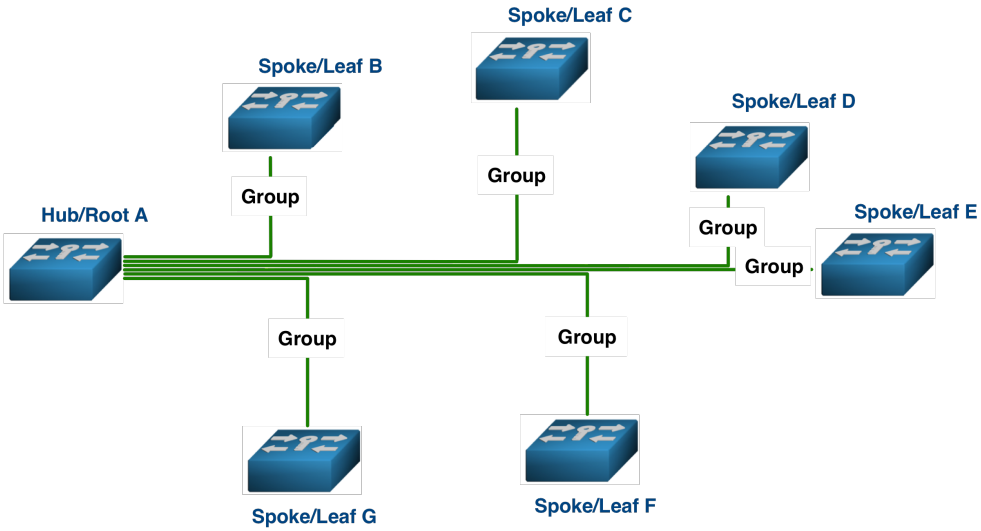
The first approach – exempting multicast and broadcast frames from encryption – leads to an inacceptable result, as there would be no security for multicast and broadcast frames. The second approach – the replication of the multicast and broadcast frames across all connections – leads to a substantial surplus load for the network. This causes either higher operating costs or a reduced network performance. Neither of those two effects can be considered desirable. The third solution – the use of a second key system – results in two different and competing key systems, but solves the problem concerning multicast and broadcast frames. Depending on the frame type the responsibility lies with one key system or the other. A group key system is used for the multicast and broadcast frames, while the pairwise key system handles the unicast frames. The fourth approach is the most efficient: A key system that can handle unicast, multicast and broadcast frames.

6.5.2. Group Keys

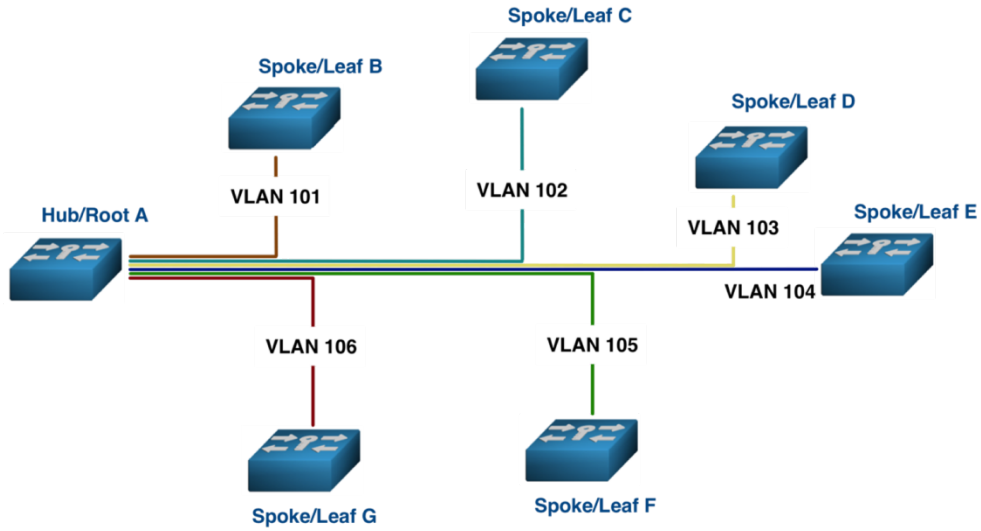
Group keys are based on the principle that for the communication within a defined group the same key is used to encrypt the communication. The membership in one group does not exclude a member from concurrent membership in other groups. For the communication within different groups different keys are used. Keys are unique to a group and separate the groups cryptographically. A group consists of two or more members. For Ethernet networks, group assignment is mostly based on the VLAN tag,

This works for all three basic topologies, starting with point-to-point:

In point-to-multipoint scenarios there are two different approaches: The network members can be treated as single group.

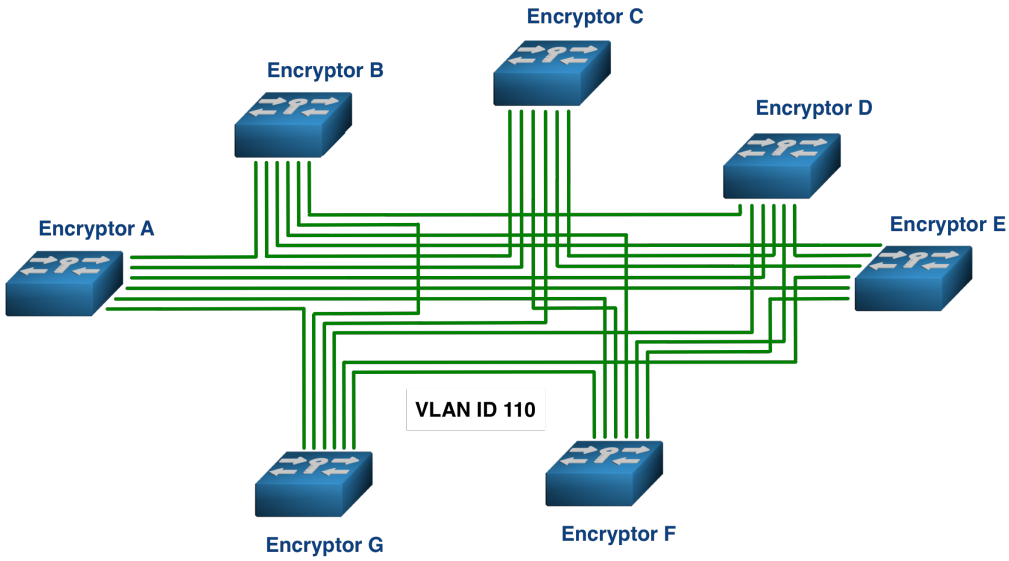


Or each connection between the hub and a spoke is treated as a single group.

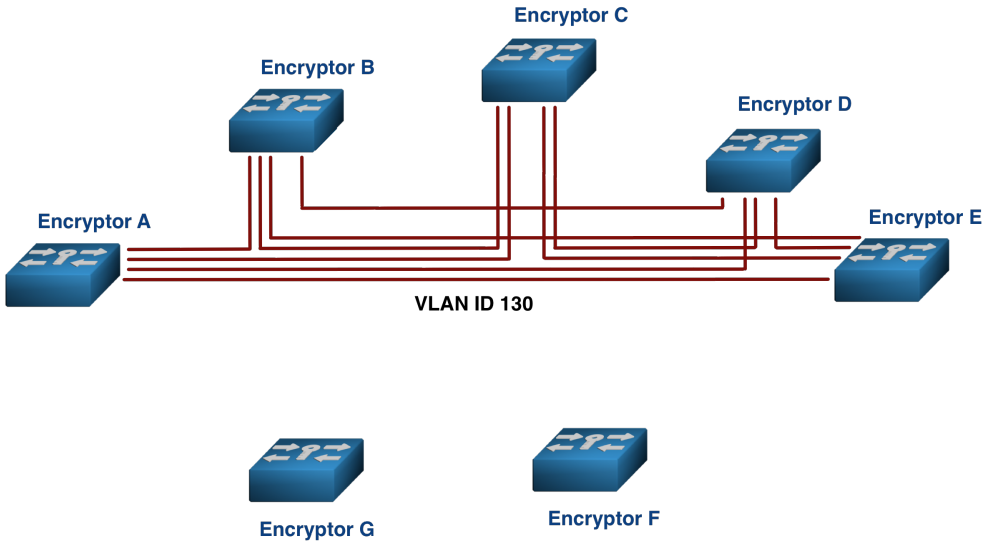


It is also possible to use a mix between the two approaches.

In multipoint-to-multipoint topologies group key system allow the layering of different groups. Such a group can e.g., consist of the members of a VLAN. If that VLAN covers all sites, then all sites are members of this group, unless specific sites are excluded despite containing members of the VLAN.



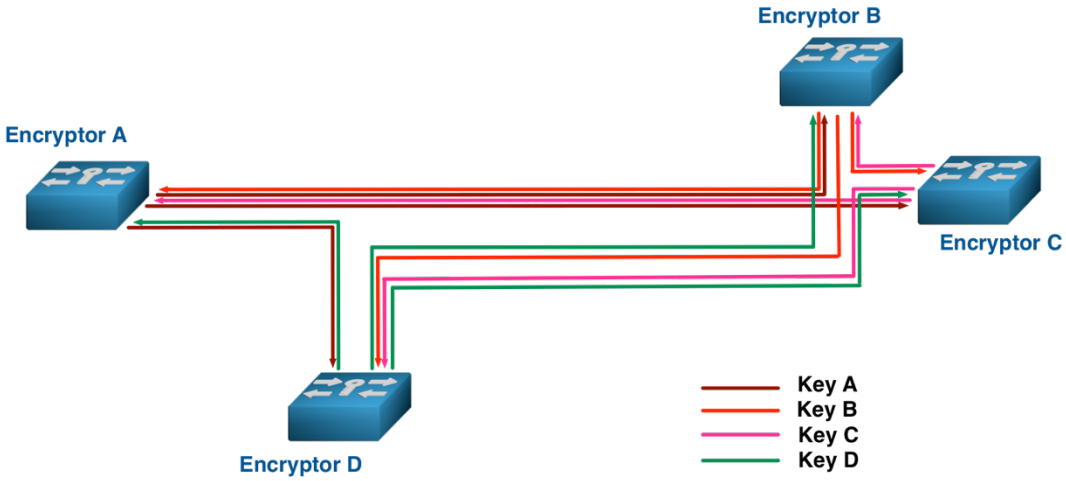
If a VLAN only covers a limited number of sites, then only these sites are member of this group.



Multipoint connections often are groups that share a common broadcast domain. Within a group all data traffic is encrypted with the same session key. There is no differentiation between unicast, multicast and broadcast frames.

Powerful group key systems allow the establishment of group membership through parameters such as VLAN-IDs. Such group key systems normally use a redundant key server setup or are set up in a distributed way. The key server takes care of providing the right group keys to each participating encryptor, so that the group members can communicate across sites. Another task of the key server is to ensure that a new key is generated and put in use if there is any change in the membership of the group. With the new key the old data traffic cannot be decrypted and with the old key the new data traffic cannot be decrypted. This is also known as perfect forward and perfect backwards secrecy.
For Ethernet networks, it seems to be a natural fit to organize the groups according to VLAN-IDs as corporate networks tend to limit the broadcast domains by using VLANs and use those VLANs also to segment the network. A group key encryption that uses the VLAN-IDs for group membership reinforces that segmentation and establishes a cryptographic separation of the VLANs.

Not all group key systems use bidirectional keys for the encryption of the data traffic. It is also possible to use unidirectional group keys. In such group key system, the sending encryptor generates the key he will use for encrypting the outgoing frames and distributes this key to all group members that are part of his group. As every group member is also a sending encryptor, every group member distributes the key he is using for encrypting his outgoing data traffic to all other group members. In such a scenario, each encryptor is also the key server for his keys.



Each platform vendor uses a different key system and thus a different approach. Some key systems are rather device-oriented whereas others additionally offer support for existing network hierarchies and structure. Full multi-tenancy support requires support for network hierarchies, structures and segmentation combined with a group key system with distributed key servers combined with full key ownership – including initial secrets – by the tenant.

7. Network Support

7.1. Bump-in-the-Wire Deployment

Bump-in-the-wire deployment capability characterizes an encryptor that can be added to a network without requiring changes in the network infrastructure.

7.2. Jumbo Frames

The support of jumbo frames should be a matter of course (>1500 bytes) as it is a standard feature of Ethernet network interfaces. Jumbo Frames are normally used at bandwidths of 100Mbit/sec and higher.

http://en.wikipedia.org/wiki/Jumbo_frames

7.3. Ethernet Flow Control

Ethernet Flow Control supports lossless transmission by regulating the traffic flow to avoid dropped frames in case of congestion. This is done by pausing and resuming the network traffic between two nodes on a full-duplex Ethernet network. Flow control prevents buffer overflow on the two involved encryptors. Buffer overflow causes dropped frames. The PAUSE command can stop the transmission of data temporarily to avoid congestion.

http://en.wikipedia.org/wiki/Ethernet_flow_control
http://datacenteroverlords.com/2013/02/02/ethernet-congestion-drop-it-or-pause-it/

8.4 Tagging frames without a tag

In scenarios where both, frames with a VLAN tag and frames without a VLAN tag, are sent to the WAN, the encryptor can tag frames without a tag.

7.4. Fragmentation

Fragmentation/defragmentation for Ethernet works differently than the fragmentation of IPv4. It helps where the frame would exceed an MTU (Maximum Transfer Unit) size of 1500 bytes, respectively another MTU size defined by the network. Most Carrier Ethernet networks do not have any issue with an additional overhead of up to 32 bytes. Additionally, there is the possibility to use an upstream traffic shaper to reduce the frame size to the maximum allowed. If the communication is between IPv6 devices, the reduction occurs automatically.

7.5. Dead Peer Detection

The function „dead peer detection“ enables the encryptor to find out and alert if the remote station stops working.

7.6. Optical Loss Pass-Through

Optical loss-pass-through (also known as link loss return) supports the discovery of link problems on the fiber port. If the receiver of the fiber port gets no valid link signal, the sender of the fiber port suspends his activity. This function permits a switch or router to see through the encryptor and thus check if the connection to the switch or router behind the encryptor on the remote side of the connection works properly.

7.7. Link Loss Carry Forward

Link loss carry forward only sends a link signal if a link signal is received. The loss of the link is passed on to the switch or router, so that it becomes immediately known. The output port of the encryptor only sends a link signal if he gets a link signal on the input port and the input port of the encryptor only sends a link signal if he gets a link signal on the output port.
Link loss carry forward can be used for fiberoptic and copper networks.

8. System Management

8.1. Out-of-Band Management

It is necessary to be able to configure and control the encryptor. For out-of-band management a separate Ethernet port and a serial port are standard.

http://en.wikipedia.org/wiki/Out-of-band_management

8.2. In-Band Management

In-band management of the encryptors can be supported by using methods such as SSH (Secure Shell), TLS, Corba/TLS, SNMP or by using proprietary protocols.

http://en.wikipedia.org/wiki/Secure_Shell

8.3. Slots and Ports

It is necessary to be able to configure and control the encryptor. For out-of-band management a separate Ethernet port and a serial port are standard.

8.4. SNMP

All vendors support the monitoring of the encryptors in the network using SNMP. It is important to realize that SNMP is only halfway secure and supports the 64 bit counters required for high-speed network devices from version 2c on. Encryption is only supported in v3.

http://en.wikipedia.org/wiki/SNMP

The monitoring of the link status requires that the encryptor continuously publishes his operating status. SNMP monitoring software can read and process these status reports and thus monitor the current link status. This can be accomplished by setting SNMP traps for the uplink and the downlink.

8.5. Logs

The event log registers all events and is local.
The audit log registers all events that are relevant for the audit and stores them locally.
Syslog registers system messages. UDP is used for the transmission between Syslog server and encryptor, which means that neither transmission nor registration of the data is guaranteed. For that reason, the encryptor needs the local event and audit logs. Syslog support also permits to integrate the encryptors into centralized log management environments.

http://en.wikipedia.org/wiki/Computer_data_logging
http://en.wikipedia.org/wiki/Audit_trail
http://en.wikipedia.org/wiki/Syslog

9. Unit

9.1. Rack Unit

The rack unit refers to the height that the unit occupies in a standard 19“ rack. 1U stands for one rack unit and single-height, whereas 2U stands for two rack units and double height.

http://en.wikipedia.org/wiki/Rack_unit

9.2. Device Access

The rack unit refers to the height that the unit occupies in a standard 19“ rack. 1U stands for one rack unit and single-height, whereas 2U stands for two rack units and double height.

9.3. Redundant Power Supplies

Encryptors are an important part of the IT infrastructure. It is common to connect those devices to two different power circuits, so that there is no interruption in case of one of the power circuits going down.
Redundant power supplies can be connected to two different power circuits. If they are hot-swappable, they can be exchanged during operation. The power supplies used by the encryptors normally have a MTBF that is substantially higher than the MTBF of the device itself. This makes the actual breakdown of a power supply statistically very unlikely.

http://en.wikipedia.org/wiki/Uninterruptible_power_supply

9.4. Mean Time between Failures

MTBF indicates the theoretical duration between two failures. The higher the value, the lower the theoretical operating cost. One could argue that minimum values above 60'000 hours show overly inflationary tendencies, especially as these are not proven, but calculated theoretical values.

http://en.wikipedia.org/wiki/MTBF

9.5. High Availability

High availability functionality permits the redundant layout of the encryptors.

http://en.wikipedia.org/wiki/High-availability_cluster

9.6. Device Protection

Tamper evident and tamper resistant are the two different categories used for the casing. Tamper resistant is much harder to accomplish and thus more expensive. Tamper evident can be accomplished with a seal consisting of a sticker.

http://en.wikipedia.org/wiki/Tamper_proof
http://en.wikipedia.org/wiki/Tamper_evident

9.7. Security Approvals

There are many different IT security guidelines for encryption products. Some are international, some are national and others are international but use national criteria. Some countries have defined their own requirements for IT security for encryptors. In these countries, a certification for fulfilling these requirements is a precondition for the sale of such a product to governments or administrations. Most of these certifications only have limited benefit for the customers as often neither the requirements nor the depth of the examination provides a sufficient security. It is up to the customer to read the protection profile and the certification report in full detail and make the comparison with his own security requirements. It is important to understand and take into consideration that certification standards such as US Common Criteria using standardized protection profiles for EAL2+ are not driven by state-of-the art security. Most often, commercial interest of US-based vendors, certification labs, and certification consultants combined with national interests play a more important role than basic security requirements.

A certification of devices for government use for classified data by state organizations tends to have more value than a certification by commercial service providers, as the devices must meet the requirements for classified government networks. In real life those certifications do not guarantee absolute security either. For all certifications, what matters is who examined and tested what, where, and how and according to which protection profile and guidelines.

https://www.uebermeister.com/en/news-and-articles/detail/why-the-most-prevalent-it-security-certifications-such-as-fips-common-criteria-and-niap-do-not-guarantee-security

Frameworks, standards and guidelines are issued by different national and international organizations. It is preferable, if a product is not limited to the national standards of a single country, but supports a range of internationally accepted standards.

http://en.wikipedia.org/wiki/Common_Criteria
http://en.wikipedia.org/wiki/Bundesamt_für_Sicherheit_in_der_Informationstechnik
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306
http://en.wikipedia.org/wiki/FIPS_140
http://www.etsi.org/technologies-clusters/clusters/security

9.8. Security Relevant Approvals

Next to the actual security certifications there are also security relevant approvals. These cover the areas of operational security and emissions.

http://en.wikipedia.org/wiki/European_standards
http://en.wikipedia.org/wiki/List_of_EN_standards
http://en.wikipedia.org/wiki/FCC

10. Management Software

The management software supplied with the encryptors depends on the approach and feature set used by each vendor. The feature set and the functionalities to be managed decide what has to be supported by the software. Embedded web servers are harder to secure than standalone applications. The management software is an essential part of the overall security of a solution. It is therefore important to verify that for a certification the management software has been in scope and not out of scope.

10.1. Management Access

Not everybody needs to have access to all the different management functions, especially if you want to keep network and security management separated. Such a separation is a precondition for Managed Security Services and Managed Encryption Services. The authentication of the user is based on the user identity, while the access is granted according to the role of the user. Typical roles include crypto officer, network management, maintenance and user). A minimum number of two hierarchy levels of roles is required.

A strict internal separation of users is difficult to achieve, as it also requires a separate memory space for each user.

http://en.wikipedia.org/wiki/Role-based_access_control

10.2. Device Management

This category covers device management, device diagnostics, network diagnostics and link monitoring.

Device diagnostic utilities provide the health status of the device and help to pinpoint problem areas, while network diagnostics are needed to monitor and troubleshoot network connections. A remote update/upgrade facility allows keeping the devices up-to-date without local intervention.

10.3. Certificate Authority and Management

Pre-shared keys can be a viable alternative to the use of certificates and a PKI and even have some distinct advantages if implemented properly. Products that are using certificates need a certificate authority (CA), so that the required X.509 certificates can be created independently of an existing CA structure. The certificate management must cover creation, issue, revocation, etc. of certificates.
The use of non-standard X.509 certificates prevents the use of an existing CA infrastructure for the encryptors.

http://en.wikipedia.org/wiki/Certificate_authority

10.4. Key Management

Key management is responsible for the generation and management of the master and session keys, selective encryption and key assignment.
For group key systems, it also includes the group creation, group isolation and the fail-over configuration.

http://en.wikipedia.org/wiki/Key_management

11. Price and Warranty

11.1. Price

Most vendors do not want to publish their prices. Therefore, the price ranges for individual devices are shown below. Project prices vary depending on the size of the project. Prices are not necessarily proportional to the functionality and quality of a device. Some vendors compensate for excessive list prices with appropriate discounts, while others work with realistic list prices and correspondingly low discount rates. In the end, it is the price paid that is decisive and not the amount of the discount granted. The costs of maintenance contracts are usually based on the list prices, not on the prices actually paid. Those prices are for complete and secure systems, including authentication (zero trust), firewall at network layer, key management and line-rate encryption.

- for 19" devices with a full duplex throughput of 100G they are between €70'000 and €95'000
- for 19" devices with a full duplex throughput of 40G they are between €40'000 and €49'000
- for 19” devices with a full duplex throughput of 10G per port and multiple ports, they are between €24'000 and €49'000
- for 19” devices with a full duplex throughput of 10G between €24'000 and €30'000.
- for 19" devices with a full duplex throughput of 1G they are between €13'000 and €20'000, and
- prices for 100M solutions range between €4'500 and €9'000

Compact units with external power supply are priced between 20-50% lower than 19" units with redundant power supply, depending on the vendor.

11.2. Operating Cost

The price paid for the unit is just one element on the cost side. With an average operating life of 6-8 years or more, the operating cost make up for an important part of the overall cost. The operating cost themselves consist of direct operating cost of the unit (warranty, warranty coverage, warranty extension, SLA, etc.) and the line cost paid to the telecom operator. Devices that support line consolidation might reduce line cost substantially. If costs are calculated properly, line cost is an important cost element.
Operating cost is harder to calculate than the device cost, as opportunity cost has to be taken into consideration as well. E.g., if more expensive networks have to be used because the encryptor doesn’t function properly with a less costly transport network.

11.3. Warranty and Warranty Coverage

Vendors differ in terms of warranty period and warranty and maintenance coverage included in the purchase price. Different cost structures can account for hidden price differences of 10-20%.

The author would like to thank all the people that made this market overview possible:

Michael Braun (atmedia), Joerg Friedrich (atmedia), Gabi Gerber (Security Interest Group Switzerland/SIGS), Andreas Graubner (Rohde & Schwarz), Harald Herrmann (Rohde & Schwarz), Christoph Hugenschmidt (Inside-IT), Felix Jaggi, Denis Kolegov, Ronald Kuhls (Rohde & Schwarz), Ivan Pepelnjak (IPSpace.net), David Musteka (Secunet), Peter Rost (Secunet), and the countless other people, who supported this project in one way or another.

The full version of the market overview is available for a fee to qualified organizations upon request directly from the author.

Chapter 3: Tables

The tables as filled out by the vendors or as defined by MACsec.

All of the vendors listed did get the form to fill out. For vendors who decided not to fill out the form, there is an empty form that can be used with that vendor for an RFI.

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

atmedia

	Virtual Appliance	A100MC	A100M	A100MF	A1G	A10G	A4x10G	A40G	A100G
Line Interface/Supported Line Rates									
10 Mbs	✓	✓/RJ45	✓/RJ45	✓/SFP	✓/SFP				
100 Mps	✓	✓/RJ45	✓/RJ45	✓/SFP	✓/SFP	✓/SFP+			
1 Gbps	✓	✓/RJ45	✓/RJ45	✓/SFP	✓/SFP	✓/SFP+	✓/SFP+		
4 x 1 Gbps	✓								
10 Gbps	✓				✓/SFP+	✓/SFP+	✓/SFP+	✓/QSFP+	✓/QSFP28
25 Gps	✓								✓/QSFP28
4 x 10 Gbps	✓						✓/SFP+		
40 Gbps	✓							✓/QSFP+	✓/QSFP28
100 Gbps	✓								✓/QSFP28
Virtual Appliance	✓								
Supported Network Topologies (single-port)									
Point-to-Point (P2P)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Point-to-Multipoint (P2MP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multipoint (MP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supported Network Topologies (multi-port/per port)									
Point-to-Point (P2P)							✓		
Point-to-Multipoint (P2MP)							✓		
Multipoint (MP)							✓		
Supported Metro Ethernet Topologies									
Port-based									
Ethernet Private Line (EP-Line)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Private Tree (EP-Tree)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Private LAN (EP-LAN)	✓	✓	✓	✓	✓	✓	✓	✓	✓
VLAN-based									
Ethernet Virtual Private Line (EVP-Line)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Virtual Private Tree (EVP-Tree)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Virtual Private LAN (EVP-LAN)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supported Networks (Encryption)									
Ethernet	✓	✓	✓	✓	✓	✓	✓	✓	✓
MPLS (MPLSoE)	✓	✓	✓	✓	✓	✓	✓	✓	✓
MPLS (MPLSoIP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv4	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supported Networks (Transport of Encrypted Frame)									
Ethernet (native)	✓	✓	✓	✓	✓	✓	✓	✓	✓
MPLS (EoMPLS)	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv4 (including EoIP and MPLSoIP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
TCP	✓	✓	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 (including EoIP and MPLSoIP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
TCP	✓	✓	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supported Usage Scenarios									
Single tenant	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multi-tenant	✓	✓	✓	✓	✓	✓	✓	✓	✓
per port	✓	✓	✓	✓	✓	✓	✓	✓	✓
per VLAN	✓	✓	✓	✓	✓	✓	✓	✓	✓
Self-managed	✓	✓	✓	✓	✓	✓	✓	✓	✓
Managed encryption service	✓	✓	✓	✓	✓	✓	✓	✓	✓
Managed security service	✓	✓	✓	✓	✓	✓	✓	✓	✓

Platform

Platform used									
	Mainboard/Firmware	atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia	atmedia
	Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Operating Modes									
	Line Mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Multipoint Mode	✓	✓	✓	✓	✓	✓	✓	✓	✓

Data Plane Encryption Standard and Processing

Encryption Standard									
	Block Cipher	AES	AES	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Alternative Mode of Operation									
	Key Length (in bit)	256	256	256	256	256	256	256	256	256
Processing Method									
	cut-through	✓	✓	✓	✓	✓	✓	✓	✓	✓
	store&forward	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware									
	FPGA		✓	✓	✓	✓	✓	✓	✓	✓
	ASIC	✓								
	CPU	✓								
Latency									
Latency P2P Mode	cut-through	N/A	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs	<2µs
	store & forward	N/A	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs	<2µs
Latency MP Mode	cut-through	N/A	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs	<2µs
	store & forward	N/A	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs	<2µs
Performance Documentation									
Ethernet Throughput & Latency Data available		✓	✓	✓	✓	✓	✓	✓	✓	✓
RFC 2544 Throughput & Latency Data available		✓	✓	✓	✓	✓	✓	✓	✓	✓

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10	10	10
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Frame overhead (authenticated encryption)	20/28	20/28	20/28	20/28	20/28	20/28	20/28	20/28	20/28
	Ethernet multi-hop support	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Transport (Payload only)		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Max. number of peers	1000	1000	1000	1000	1000	1000	1000	1000	1000
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	256	unlimited	256	unlimited	256	unlimited	256	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Definable encryption offset (fixed)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Variable encryption offset	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Adaptive encryption offset based on frame content	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Registered EtherType	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	20/28	20/28	20/28	20/28	20/28	20/28	20/28	20/28	20/28
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tunnel (Ethernet over Ethernet)		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Max. number of peers	32	32	32	32	32	32	32	32	32
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓	✓	✓

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP
Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Replay protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
Registered Ethertype	✓	✓	✓	✓	✓	✓	✓	✓	✓
Counter length (in bytes)	10	10	10	10	10	10	10	10	10
Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*
Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓	✓	✓

Native IP Encryption

Supported IP versions									
IPv4	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supported transmission protocols									
TCP	✓	✓	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transport Mode									
Maximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
Additional Authenticated Data (header)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Replay Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
Counter length (in bytes)	10	10	10	10	10	10	10	10	10
Packet overhead authenticated encryption (AE)	20/28	20/28	20/28	20/28	20/28	20/28	20/28	20/28	20/28
Transport Tunnel Mode									
Maximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16	8/16
Additional Authenticated Data (header)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Replay Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
Counter length (in bytes)	10	10	10	10	10	10	10	10	10
Packet overhead authenticated encryption (AE)	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68

Selective Processing (Encryption, Pass, Discard)

Based on MAC Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on VLAN ID	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on Ethertype	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on Multicast Group	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on Presence of MPLS Tag	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on IP Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
Combination of multiple selection criteria	✓	✓	✓	✓	✓	✓	✓	✓	✓

Mixed Ethernet, MPLS, EoIP and IP Support

Based on VLAN ID									
MPLS	✓	✓	✓	✓	✓	✓	✓	✓	✓
EoIP	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on presence of MPLS tag									
MPLS	✓	✓	✓	✓	✓	✓	✓	✓	✓
EoIP	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP	✓	✓	✓	✓	✓	✓	✓	✓	✓
Based on VLAN ID and presence of MPLS tag									
MPLS	✓	✓	✓	✓	✓	✓	✓	✓	✓
EoIP	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP	✓	✓	✓	✓	✓	✓	✓	✓	✓

Extended Security Features									
AES S-box customization									
Customizable AES S-box		✓	✓	✓	✓	✓	✓	✓	✓	✓
Traffic Masking									
Method									
	Fixed MTU size	N/A**	✓	✓	✓	✓	✓	✓	✓	✓
	Synthetic traffic injection	N/A**	✓	✓	✓	✓	✓	✓	✓	✓
Supported topologies									
	P2P	N/A**	✓	✓	✓	✓	✓	✓	✓	✓
	P2MP	N/A**	✓	✓	✓	✓	✓	✓	✓	✓
Control Plane Options and Security									
Control Plane Options									
	In-band	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Out-of-band	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Option to separate key exchange from control plane	✓	✓	✓	✓	✓	✓	✓	✓	✓
Protection layer (in-band)									
	Ethernet (layer 2)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP (layer 3)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Transport (layer 4)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware (in-band)									
	FPGA		✓	✓	✓	✓	✓	✓	✓	
	ASIC	✓								✓
	CPU	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption (in-band)									
	Separate from data plane encryption	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Same protection level as data plane encyption	✓	✓	✓	✓	✓	✓	✓	✓	✓
DoS Resiliency (in-band)									
	line rate		✓	✓	✓	✓	✓	✓	✓	✓
Auto-discovery									
Auto-discovery of network encryptors		✓	✓	✓	✓	✓	✓	✓	✓	✓
Auto-discovery of key servers		✓	✓	✓	✓	✓	✓	✓	✓	✓
Auto-discovery of VLANs		✓	✓	✓	✓	✓	✓	✓	✓	✓
Disabling of auto-discovery		✓	✓	✓	✓	✓	✓	✓	✓	✓
Key Server									
Integrated Key Server		✓	✓	✓	✓	✓	✓	✓	✓	✓
Support for external Key Server		✓	✓	✓	✓	✓	✓	✓	✓	✓
External Key Server										
Support for multiple distributed Key Servers		✓	✓	✓	✓	✓	✓	✓	✓	✓
Support for fail-over to back-up Key Server		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Number of backup key servers									
	Number of hierarchy levels of backup key servers									
Autonomous operation		✓	✓	✓	✓	✓	✓	✓	✓	✓
Key Management									
Key Generation and Storage									
Hardware Random Number Generation		with SC/HSM	✓	✓	✓	✓	✓	✓	✓	✓
Tamper Security Key Storage (tamper-evident or tamper-proof)		with SC/HSM: TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)									
Elliptic Curve Cryptography (ECC)									
	Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521	512/521	512/521
	Key strength (in bit)	256	256	256	256	256	256	256	256	256
Supported Curves:										
	NIST	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Brainpool	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Custom Curves	✓	✓	✓	✓	✓	✓	✓	✓	✓

Hash Algorithms										
SHA-2	Key length	512	512	512	512	512	512	512	512	512
	Key strenght (Image/Collision Resistance)	512/256	512/256	512/256	512/256	512/256	512/256	512/256	512/256	512/256
CBC-MAC-GCM										
	Key length	256	256	256	256	256	256	256	256	256
	Key strength	256	256	256	256	256	256	256	256	256
Device Authentication										
Symmetric Signature: Pre-shared Key (PSK)		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
	Key length	256	256	256	256	256	256	256	256	256
	Key strenght (in bit)	256	256	256	256	256	256	256	256	256
Asymmetric Signature: Certificate		optional	optional	optional	optional	optional	optional	optional	optional	optional
	Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
	Key lenght	512	512	512	512	512	512	512	512	512
	Key strenght (in bit)	256	256	256	256	256	256	256	256	256
Ad-hoc authentication of peers (manual)		✓	✓	✓	✓	✓	✓	✓	✓	✓
Signature key protocol		AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****
Key Agreement and Key Exchange										
Master Key (KEK) Agreement		ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key		✓	✓	✓	✓	✓	✓	✓	✓	✓
Minimum suggested Time Interval for Master Key Change (min)		60	60	60	60	60	60	60	60	60
Separate Master Key (KEK) per site		✓	✓	✓	✓	✓	✓	✓	✓	✓
Separate Master Key (KEK) per group		✓	✓	✓	✓	✓	✓	✓	✓	✓
Session Key (DEK) Exchange Agreement		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys		✓	✓	✓	✓	✓	✓	✓	✓	✓
Minimum Time Interval for Session Key Change (min)		1	1	1	1	1	1	1	1	1
Quantum-safe Key Exchange										
Symmetric Encryption of Asymmetric Key Exchange		✓	✓	✓	✓	✓	✓	✓	✓	✓
QKD (optical short range only)										
Quantum-safe Key Exchange Algorithm		✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)	✓ (Frodo; on-demand)
Key Exchange Options										
In-band		✓	✓	✓	✓	✓	✓	✓	✓	✓
Out-of-band		✓	✓	✓	✓	✓	✓	✓	✓	✓
Key exchange via raw Ethernet		✓	✓	✓	✓	✓	✓	✓	✓	✓
In-band key exchange via IP	IPv4	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IPv6	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key System										
Point-to-Point Key System										
Supported key system										
	Pairwise	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:										
	MAC Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
Point-to-Multipoint Key System										
Supported key systems:										
	Pairwise	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:										
	MAC Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓	✓	✓

Multipoint Key System									
Supported key systems:									
	Pairwise	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
	Mixed (pairwise unicast, group multicast)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key assignment based on:										
	MAC address (pairwise and mixed)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Multicast groups (mixed)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VLAN ID (group)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group (group)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Multicast Group	✓	✓	✓	✓	✓	✓	✓	✓	✓
Individual key per multicast group		✓	✓	✓	✓	✓	✓	✓	✓	✓
Individual key per broadcast group (VLAN ID)		✓	✓	✓	✓	✓	✓	✓	✓	✓
Group Key System Specifics										
Additional separate authentication per group		✓	✓	✓	✓	✓	✓	✓	✓	✓
Group Membership Definition										
	Multicast group membership	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Individual membership	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Network membership	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VLAN membership	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Trunked VLAN membership	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exclusion										
	MAC address	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Frames with MPLS tag	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IP Muticast Group	✓	✓	✓	✓	✓	✓	✓	✓	✓
Group Key Distribution										
	Unicast (unique KEK per group member)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Broadcast (same KEK for all group members)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network Support										
Bump in the Wire deployment		✓	✓	✓	✓	✓	✓	✓	✓	✓
Jumbo Frame Support		✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Flow Control via PAUSE		✓	✓	✓	✓	✓	✓	✓	✓	✓
Tagging of untagged frames		✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Fragmentation/Defragmentation		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Point-to-Point	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Point-to-Multipoint	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Multipoint	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dead Peer Detection		✓	✓	✓	✓	✓	✓	✓	✓	✓
Optical Loss Pass-Through		N/A	N/A	N/A	N/A	✓	✓	✓	✓	✓
Link Loss Carry Forward		N/A	✓	✓	✓	N/A	N/A	N/A	N/A	N/A
System Configuration and Management Access										
IPv4		✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv6		✓	✓	✓	✓	✓	✓	✓	✓	✓
Out-of-band Management		✓	✓	✓	✓	✓	✓	✓	✓	✓
	RS-232/V.24	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Separate Ethernet port	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart Card (Secure Card) Support		✓	✓	✓	✓	✓	✓	✓	✓	✓
USB Port		✓						✓	✓	✓
In-band Management		✓	✓	✓	✓	✓	✓	✓	✓	✓
	SSH	✓	✓	✓	✓	✓	✓	✓	✓	✓
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only	read-only	read-only	read-only
	TLS									
	Proprietary	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote Monitoring (SNMP)		v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3
Logs										
Event Log (local)		✓	✓	✓	✓	✓	✓	✓	✓	✓
Audit Log (local)		✓	✓	✓	✓	✓	✓	✓	✓	✓
Syslog Support (Server)		✓	✓	✓	✓	✓	✓	✓	✓	✓

Unit

Height in 19" Rack	N/A	1U	1U	1U	1U	1U	1U	1U	1U
Number of external encrypted Ethernet ports	unrestricted	1	1	1	1	1	1-4	1-4	1-4
Physical Device Access	N/A	back	back	front	front	front	front	front	front
Redundant Power Supply	dependent on server			✓	✓	✓	✓	✓	✓
Redundant, hot-swappable power supply	dependent on server			✓	✓	✓	✓	✓	✓
High Availability functionality (two-node cluster)	1:1	1:1	1:1	1:1	1:1	1:1	1:1	1:1	1:1
MTBF	N/A	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
Tamper Security	N/A	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	N/A			BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL)					
Safety Approvals	N/A			EN55032 Class B, FCC Part 15 Class B, ROHS					
Boot Time									
Cold boot until operational (P2P)	N/A	25s	25s	25s	25s	25s	25s	25s	25s
Warm boot until operational (P2P)	N/A	27s	27s	27s	27s	27s	27s	27s	27s

Management Software

User Interface: Native PC application	✓	✓	✓	✓	✓	✓	✓	✓	✓
Embedded Webapp									
CLI	✓	✓	✓	✓	✓	✓	✓	✓	✓
Initial Device Set-up									
Local (out-of-band)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote (out-of-band)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Configuration									
Local (out-of-band)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote (in-band)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote (out-of-band)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Management Access									
Role-based access	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity-based authentication of user	✓	✓	✓	✓	✓	✓	✓	✓	✓
Number of hierarchy levels	2	2	2	2	2	2	2	2	2
Number of roles	5	5	5	5	5	5	5	5	5
Strict internal separation of users	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Management									
Device Diagnostics	✓	✓	✓	✓	✓	✓	✓	✓	✓
Link Monitoring (SNMP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Connection Diagnostics	✓	✓	✓	✓	✓	✓	✓	✓	✓
In-band Network Diagnostics	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote Update/Upgrade	✓	✓	✓	✓	✓	✓	✓	✓	✓
Certificate Authority & Management	optional	optional	optional	optional	optional	optional	optional	optional	optional
Certificate Creation	optional	optional	optional	optional	optional	optional	optional	optional	optional
Certificate Management	optional	optional	optional	optional	optional	optional	optional	optional	optional
Key Management									
Group creation	✓	✓	✓	✓	✓	✓	✓	✓	✓
Group isolation	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fail-over configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓

Price

List Price Encryption Unit (in €)	on request	on request	on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement	on request	on request	on request	on request	on request	on request	on request	on request	on request
Required Management Software									
2-10 encryptors	included	included	included	included	included	included	included	included	included
11-25 encryptors	included	included	included	included	included	included	included	included	included
26-50 encryptors	included	included	included	included	included	included	included	included	included
51+ encryptors	included	included	included	included	included	included	included	included	included
Warranty Period (months)	24	24	24	24	24	24	24	24	24
Warranty Coverage: Parts & Work	✓	✓	✓	✓	✓	✓	✓	✓	✓
Basic Support (9 to 5, e-mail, phone)	on request	on request	on request	on request	on request	on request	on request	on request	on request
Software updates and upgrades	on request	on request	on request	on request	on request	on request	on request	on request	on request
Warranty Extension (per year)	on request	on request	on request	on request	on request	on request	on request	on request	on request

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

Rohde & Schwarz

	SITLine ETH50	SITLine ETH4G	SITLine ETH40G	SITLine ETH-S	SITLine ETH-L	SITLine ETH-XL	SITLine IP 100M	SITLine IP1G	SITLine IP10G
Line Interface/Supported Line Rates									
10 Mbs	✓	✓		✓		✓	✓	✓	
100 Mps	✓	✓		✓		✓	✓	✓	
1 Gbps		✓		✓		✓		✓	
4 x 1 Gbps		✓				✓ (2x)			
10 Gbps			✓		✓	✓			✓
4 x 10 Gbps			✓		✓	✓ (2x)			
25 Gps									
40 Gbps									
100 Gbps						✓ (2x)			
Virtual Appliance	-	-	-	-	-	-		-	-
Supported Network Topologies (single-port)									
Point-to-Point (P2P)	✓	✓	✓	✓	✓	✓		✓	✓
Point-to-Multipoint (P2MP)	✓	✓	✓	✓	✓	✓		✓	✓
Multipoint (MP)	✓	✓	✓	✓	✓	✓		✓	✓
Supported Network Topologies (multi-port/per port)									
Point-to-Point (P2P)		✓	✓		✓	✓			
Point-to-Multipoint (P2MP)		✓	✓		✓	✓			
Multipoint (MP)		✓	✓		✓	✓			
Supported Metro Ethernet Topologies									
Port-based									
Ethernet Private Line (EP-Line)	✓	✓	✓	✓	✓	✓			
Ethernet Private Tree (EP-Tree)	✓	✓	✓	✓	✓	✓			
Ethernet Private LAN (EP-LAN)	✓	✓	✓	✓	✓	✓			
VLAN-based									
Ethernet Virtual Private Line (EVP-Line)	✓	✓	✓	✓	✓	✓			
Ethernet Virtual Private Tree (EVP-Tree)	✓	✓	✓	✓	✓	✓			
Ethernet Virtual Private LAN (EVP-LAN)	✓	✓	✓	✓	✓	✓			
Supported Networks (Encryption)									
Ethernet	✓	✓	✓	✓	✓	✓			
MPLS (MPLSoE)	✓	✓	✓	✓	✓	✓			
MPLS (MPLSoIP)									
IPv4							✓	✓	✓
IPv6							✓	✓	✓
Supported Networks (Transport of Encrypted Frame)									
Ethernet (native)	✓	✓	✓	✓	✓	✓			
MPLS (EoMPLS)	✓	✓	✓	✓	✓	✓			
IPv4 (including EoIP and MPLSoIP)									
TCP							✓	✓	✓
UDP							✓	✓	✓
IPv6 (including EoIP and MPLSoIP)									
TCP							✓	✓	✓
UDP							✓	✓	✓
Supported Usage Scenarios									
Single tenant	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multi-tenant									
per port									
per port per VLAN									
Self-managed	✓	✓	✓	✓	✓	✓	✓	✓	✓
Managed encryption service	✓	✓	✓	✓	✓	✓	✓	✓	✓
Managed security service	✓	✓	✓	✓	✓	✓	✓	✓	✓

Platform

Platform used

Mainboard/Firmware	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S
Key Management	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S

Operating Modes

Line Mode	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S
Multipoint Mode	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S	R&S

Data Plane Encryption Standard and Processing

Encryption Standard

Block Cipher	AES	AES	AES	AES	AES	AES	AES	AES	AES
Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
Alternative Mode of Operation									
Key Length (in bit)	256	256	256	256	256	256	256	256	256

Processing Method

cut-through		✓	✓			✓			
store&forward	✓	✓	✓	✓	✓	✓	✓	✓	✓

Encryption Hardware

FPGA	✓	✓	✓	✓	✓	✓	✓	✓	✓
ASIC									
CPU									

Latency

Latency P2P Mode	cut-through					3µ			
	store & forward	16µ-85µ	4µ-10µ	4µ-10µ	16µ-85µ	4µ-10µ		<150µs	<35µs	<10µs
Latency MP Mode	cut-through					3µ			
	store & forward	16µ-85µ	4µ-10µ	4µ-10µ	16µ-85µ	4µ-10µ			

Performance Documentation

Ethernet Throughput & Latency Data available	✓	✓	✓	✓	✓		✓	✓	✓
RFC 2544 Throughput & Latency Data available	✓	✓	✓	✓	✓		✓	✓	✓

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)

Transport (Payload only)

Max. number of peers	256	4000	4000	1000	4000	8000			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	256	4000	4000	1000	4000	4000			
Integrity protection (algorithm)	AES-GCM	AES-GCM	AES-GCM	AES-GCM	AES-GCM	AES-GCM			
Authentication length (bytes)	8-16	8-16	8-16	8-16	8-16	8-16			
AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓			
Replay protection	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority			
Variable replay window (size)			-	-	-	-			
Definable encryption offset (fixed)	✓	✓	✓	✓	✓	✓			
Variable encryption offset	✓	✓	✓	✓	✓	✓			
Adaptive encryption offset based on frame content									
Registered EtherType	✓	✓	✓	✓	✓	✓			
Counter length (in bytes)									
Frame overhead authenticated encryption (AE)	18-26 (P2P), 28-36 (MP)	18-26 (P2P), 28-36 (MP)	18-26 (P2P), 28-36 (MP)	18-26	18-26	18-26			
Ethernet multi-hop support	✓	✓	✓	✓	✓	✓			

Tunnel (Ethernet over Ethernet)

Max. number of peers	256	4000	4000	1000	4000	8000			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	256	4000	4000	1000	4000	4000			
Integrity protection (algorithm)	AES-GCM	AES-GCM	AES-GCM	AES-GCM	AES-GCM	AES-GCM			
Authentication length (bytes) (n)	8-16	8-16	8-16	8-16	8-16	8-16			
AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓			
Replay protection	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority	3 frames per channel and priority			
Variable replay window (size)									
Registered Ethertype	✓	✓	✓	✓	✓	✓			
Counter length (in bytes)									
Frame overhead authenticated encryption (AE)	30-38	30-38	30-38	30-38	30-38	30-38			
Ethernet multi-hop support	✓	✓	✓	✓	✓	✓			

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)

Native IP Encryption										
Supported IP versions										
	IPv4							✓	✓	✓
	IPv6							✓	✓	✓
Supported transport protocols										
	TCP							✓	✓	✓
	UDP							✓	✓	✓
Transport Mode										
	Mximum number of peers							4000	4000	4000
	Maximum number of IP addresses							unlimited	unlimited	unlimited
	Maximum number of multicast groups							unlimited	unlimited	unlimited
	Integrity protection (algorithm)							AES-GCM	AES-GCM	AES-GCM
	Authentication length (bytes) (n)							8-16	8-16	8-16
	Additional Authenticated Data (header)							✓	✓	✓
	Replay Protection							✓	✓	✓
	Variable replay window (size)									
	Counter length (in bytes)							6	6	6
	Packet overhead authenticated encryption (AE)							20-28	20-28	20-28
Transport Tunnel Mode										
Selective Processing (Encryption, Pass, Discard)										
Based on MAC Address								✓	✓	✓
Based on VLAN ID								✓	✓	✓
Based on Ethertype								✓	✓	✓
Based on Multicast Group								✓	✓	✓
Based on Presence of MPLS Tag										
Based on IP Address								✓	✓	✓
Combination of multiple selection criteria								✓	✓	✓
Mixed Ethernet, MPLS, EoIP and IP Support										
Based on VLAN ID										
	MPLS									
	EoIP									
	IP									
Based on presence of MPLS tag										
	MPLS									
	EoIP									
	IP									
Based on VLAN ID and presence of MPLS tag										
	MPLS									
	EoIP									
	IP									
Extended Security Features										
AES S-box customization										
Customizable AES S-box		✓	✓	✓	✓	✓	✓	✓	✓	✓
Traffic Flow Security										
Method										
	Fixed MTU size									
	Synthetic traffic injection									
Supported topologies										
	P2P									
	P2MP									

Control Plane Options and Security

Control Plane Options										
	In-band	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Out-of-band	✓	✓							
	Option to separate key exchange from control plane Die Control Plane ist die Kommunikation der Daten zwischen den Verschlüsslern. Dazu gehört auch der Schlüsselaustausch. Man kann den Schlüsselaustausch allerdings via Management Plane auf ein anderes Netzwerk legen.und dort voerschlüsseln.									
Protection layer (in-band)										
	Ethernet (layer 2)	✓	✓	✓	✓	✓	✓			
	IP (layer 3)							✓	✓	✓
	Transport (layer 4)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware (in-band)										
	FPGA	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ASIC									
	CPU	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encryption (in-band)										
	Separate from data plane encryption	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Same protection level as data plane encyption	✓	✓	✓	✓	✓	✓	✓	✓	✓
DoS Resiliency (in-band)										
	line rate	✓	✓	✓	✓	✓	✓	✓	✓	✓

Auto-discovery

Auto-discovery of network encryptors	✓	✓	✓	✓	✓	✓			
Auto-discovery of key servers	each peer is a key server	each peer is a key server	each peer is a key server	each peer is a key server	each peer is a key server	each peer is a key server	each peer is a key server	each peer is a key server	each peer is a key server
Auto-discovery of VLANs									
Disabling of auto-discovery									

Key Server

Integrated Key Server	✓	✓	✓	x	x	x		x	x
Support for external Key Server									
External Key Server									
Support for multiple distributed Key Servers	✓	✓	✓	x	x	x		x	x
Support for fail-over to back-up Key Server	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
Number of backup key servers									
Number of hierarchy levels of backup key servers									
Autonomous operation	x	✓	✓	x	x	x		x	x

Key Management

Key Generation and Storage									
Hardware Random Number Generation	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4	TRG.3/DRG.4
Tamper Security Key Storage (tamper-evident or tamper-proof)	tamper-proof	tamper-proof	tamper-proof	tamper-proof	tamper-proof	tamper-proof	tamper-proof	tamper-proof	tamper-proof
Asymmetric Key Algorithms (Public Key Cryptography)									
RSA									
Key length									
Key strength (in bit)									
Elliptic Curve Cryptography (ECC)									
Key length	257	257	257	384/512	384/512	384/512	384/512	384/512	384/512
Supported Curves:									
NIST				✓	✓	✓	✓	✓	✓
Brainpool				✓	✓	✓	✓	✓	✓
Custom Curves	✓	✓	✓						
Hash Algorithms									
SHA-2 Key length	256	256	256	384/512	384/512	384/512	384/512	384/512	384/512
Key strenght (Image/Collision Resistance)	128	128	128	192/256	192/256	192/256	192/256	192/256	192/256

Device Authentication									
Symmetric Signature: Pre-shared Key (PSK)									
	Maximum number of PSKs per encryptor								
	Key length								
	Key strenght (in bit)								
Asymmetric Signature: Certificate		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Maximum number of certificates per encryptor	1	1	1	4	4	4	4	4	4
	Key lenght	257	257	257	384/512	384/512	384/512	384/512	384/512	384/512
	Key strenght (in bit)									
Ad-hoc authentication of peers (manual)										
Signature key protocol		EC-DSA	EC-DSA	EC-DSA	EC-DSA	EC-DSA	EC-DSA	EC-DSA	EC-DSA	EC-DSA
Key Agreement and Key Exchange										
Master Key (KEK) Agreement		EC-DH	EC-DH	EC-DH	EC-DH	EC-DH	EC-DH	EC-DH	EC-DH	EC-DH
Master Key (KEK) Exchange Protocol		EC-GDSA	EC-GDSA	EC-GDSA	EC-GDSA	EC-GDSA	EC-GDSA	EC-GDSA	EC-GDSA	EC-GDSA
Automatic Change of Master Key		✓	✓	✓	✓	✓	✓	✓	✓	✓
Minimum suggested Time Interval for Master Key Change (min)		6h	6h	6h	6h	6h	6h	10h (default)	10h (default)	10h (default)
Separate Master Key (KEK) per site		✓	✓	v	✓	✓	✓	✓	✓	✓
Separate Master Key (KEK) per group		NA	NA	NA	NA	NA	NA	NA	NA	NA
Session Key (DEK) Exchange Agreement										
Session Key (DEK) Exchange Protocol		prop	prop	prop	prop	prop	prop	prop	prop	prop
Automatic Change of Session Keys		✓	✓	✓	✓	✓	✓	✓	✓	✓
Minimum Time Interval for Session Key Change (min)		1 min	1 min	1 min	1 min	1 min	1 min	1 min	1 min	1 min
Quantum-safe Key Exchange										
Symmetric Encryption of Asymmetric Key Exchange					✓ (QKD-ready)	✓ (QKD-ready)	✓ (QKD-ready)			
QKD (optical short range only)										
Quantum-safe Key Exchange Algorithm										
Key Exchange Options										
In-band		✓	✓	✓	✓	✓	✓	✓	✓	✓
Out-of-band										
Key exchange via raw Ethernet		✓	✓	✓	✓	✓	✓			
In-band key exchange via IP	IPv4							✓	✓	✓
	IPv6							✓	✓	✓
Key System										
Point-to-Point Key System										
Supported key system										
	Pairwise	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group									
Key assignment based on:										
	MAC Address									
	VLAN ID	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓			
	Group							✓	✓	✓
	IP Address							✓	✓	✓
Point-to-Multipoint Key System										
Supported key systems:										
	Pairwise	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group
Key assignment based on:										
	MAC Address									
	VLAN ID	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓			
	Group							✓	✓	✓
	IP Address							✓	✓	✓

Multipoint Key System									
Supported key systems:									
Pairwise	✓	✓	✓	✓	✓	✓	✓	✓	✓
Group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group	unidirectional group
Mixed (pairwise unicast, group multicast)									
Key assignment based on:									
MAC address (pairwise and mixed)									
Multicast groups (mixed)									
VLAN ID (group)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Port	✓	✓	✓	✓	✓	✓	✓	✓	✓
Group (group)									
IP Address							✓	✓	✓
IP Multicast Group							✓	✓	✓
Individual key per multicast group									
Individual key per broadcast group (VLAN ID)									
Group Key System Specifics									
Additional separate authentication per group									
Group Membership Definition									
Multicast group membership							✓	✓	✓
Individual membership	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network membership							✓	✓	✓
VLAN membership							✓	✓	✓
Trunked VLAN membership									
IP Address							✓	✓	✓
Exclusion									
MAC address									
VLAN ID									
Frames with MPLS tag									
IP Address									
IP Muticast Group									
Group Key Distribution									
Unicast (unique KEK per group member)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Broadcast (same KEK for all group members)									
Network Support									
Bump in the Wire deployment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Jumbo Frame Support	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Flow Control via PAUSE				✓	✓	✓	✓	✓	✓
Tagging of untagged frames									
Ethernet Fragmentation/Defragmentation							✓	✓	✓
Point-to-Point							✓	✓	✓
Point-to-Multipoint							✓	✓	✓
Multipoint							✓	✓	✓
Dead Peer Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓
Optical Loss Pass-Through	✓	✓	✓	✓	✓	✓	✓	✓	✓
Link Loss Carry Forward	✓	✓	✓	✓	✓	✓	✓	✓	✓
System Configuration and Management Access									
Over IPv4	✓	✓	✓	✓	✓	✓	✓	✓	✓
Over IPv6				✓	✓	✓	✓	✓	✓
Out-of-band Management									
RS-232/V.24				✓		✓			
Separate Ethernet port		✓	✓	✓	✓	✓	✓	✓	✓
Smart Card (Secure Card) Support	✓	✓	✓	✓	✓	✓	✓	✓	✓
USB Port				✓	✓	✓	✓	✓	✓
In-band Management									
SSH	✓	✓	✓	✓	✓	✓	✓	✓	✓
SNMP (read-only/read-write)	✓	✓	✓	✓	✓	✓	✓	✓	✓
TLS	✓	✓	✓	✓	✓	✓	✓	✓	✓
Proprietary									
Remote Monitoring (SNMP)	✓	✓	✓	✓	✓	✓	✓	✓	✓

Logs

Event Log (local)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Audit Log (local)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Syslog Support (Server)	✓	✓	✓	✓	✓	✓	✓	✓	✓

Unit

Height in 19" Rack	1	1	1	1	1	1	1	1	1
Number of external encrypted Ethernet ports	1	1-4	1-4	1	1-4	1-8	1	1	1
Physical Device Access (front/back)	front	front	front	front	front	front	front	front	front
Redundant Power Supply	✓	✓	✓	✓	✓	✓	✓	✓	✓
Redundant, hot-swappable power supply	(x)	✓	✓	(x)	✓	✓	✓	✓	✓
High Availability functionality (two-node cluster)	NA	NA	NA	NA	NA	NA	NA	NA	NA
MTBF	350000 h	185000 h	185000 h	660000 h	98000 h		98000 h	98000 h	98000 h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	BSI, NATO, EU	BSI, NATO, EU	BSI, NATO, EU	BSI, NATO, EU	BSI, NATO, EU	BSI, NATO, EU		BSI, NATO	BSI, NATO
Safety Approvals	CE	CE	CE	CE	CE	CE		CE	CE
Boot Time									
Cold boot until operational (P2P)	2 min	1-2 min	1-2 min	1 min	1 -2 min	1 -2 min	1 -2 min	1 -2 min	1 -2 min
Warm boot until operational (P2P)	2 min	1-2 min	1-2 min	1 min	1 -2 min	1 -2 min	1 -2 min	1 -2 min	1 -2 min

Management Software

User Interface	Native PC application (applets)	✓	✓	✓					
	Embedded Webapp				✓	✓	✓	x	x	x
	CLI									
Initial Device Set-up										
	Local (out-of-band)	✓	✓	✓	✓	✓	✓	x	x	x
	Remote (out-of-band)									
Device Configuration										
	Local (out-of-band)	✓	✓	✓	✓	✓	✓	x	x	x
	Remote (in-band)	✓	✓	✓	✓	✓	✓	x	x	x
	Remote (out-of-band)	✓	✓	✓	✓	✓	✓	x	x	x
Management Access										
	Role-based access	✓	✓	✓	✓	✓	✓	x	x	x
	Identity-based authentication of user	✓	✓	✓	✓	✓	✓	x	x	x
	Number of hierarchy levels (Hierarchiestufen pro Rolle)	3	3	3	3	3	3	3	3	3
	Number of roles	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Strict internal separation of users	✓	✓	✓	✓	✓	✓	x	✓	x
Device Management										
	Device Diagnostics	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Link Monitoring (SNMP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Connection Diagnostics	✓	✓	✓	✓	✓	✓	✓	✓	✓
	In-band Network Diagnostics									
	Remote Update/Upgrade	✓	✓	✓	✓	✓	✓	✓	✓	✓
Certificate Authority & Management										
	Certificate Creation	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Certificate Management	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key Management										
	Group creation	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Group isolation				✓	✓	✓	✓	✓	✓
	Key assignment									
	Fail-over configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓

Price

List Price Encryption Unit (in €)	kA	kA	kA	kA	kA	kA	kA	kA	kA
Per external Key Server (in €); optional, no requirement									
Required Management Software	R&S SITScope	R&S SITScope	R&S SITScope	R&S Trusted Objects Manager	R&S Trusted Objects Manager	R&S Trusted Objects Manager	R&S Trusted Objects Manager	R&S Trusted Objects Manager	R&S Trusted Objects Manager
2-10 encryptors									
11-25 encryptors									
26-50 encryptors									
51+ encryptors									
Warranty Period (months)	24	24	24	24	24	24	24	24	24
Warranty Coverage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Basic Support (9 to 5, e-mail, phone, ticketsystem)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Software updates and upgrades	updates	updates	updates	updates	updates	updates	updates	updates	updates
Warranty Extension (per year)	✓	✓	✓	✓	✓	✓	✓	✓	✓

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

Secunet

	SINA L2 Box S 50M-2	SINA L2 Box S 1G-3	SINA L2 Box S 10G-3	SINA L2 Box S 4x1G SFP	SINA L2 Box S 4x10G SFP	SINA L2 Box S 40G	SINA L2 Box S 100G
Line Interface/Supported Line Rates							
10 Mbs	✓ /RJ45	✓ /RJ45					
100 Mps	✓ /RJ45	✓/RJ45 (/SFP on request)					
1 Gbps	✓ /RJ45	✓ /RJ45 (/SFP on request)	✓/SFP+	✓4x /SFP			
4 x 1 Gbps				✓4x /SFP			
10 Gbps			✓ /SFP+		✓4x /SFP+	✓/QSFP+/SFP+	
25 Gps							✓ /QSFP28
4 x 10 Gbps					✓4x /SFP+	✓/QSFP+	
40 Gbps						✓/QSFP+	✓ /QSFP28
50 Gbps							✓/QSFP28
100 Gbps							✓/QSFP28/FEC
Virtual Appliance							
Supported Network Topologies (single-port)							
Point-to-Point (P2P)	✓	✓	✓	✓	✓	✓	✓
Point-to-Multipoint (P2MP)	✓	✓	✓	✓	✓	✓	✓
Multipoint (MP)	✓	✓	✓	✓	✓	✓	✓
Supported Network Topologies (multi-port/per port)							
Point-to-Point (P2P)				✓	✓	(✓)	(✓)
Point-to-Multipoint (P2MP)				✓	✓	(✓)	(✓)
Multipoint (MP)				✓	✓	(✓)	(✓)
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✓	✓	✓	✓	✓	✓	✓
Ethernet Private Tree (EP-Tree)	✓	✓	✓	✓	✓	✓	✓
Ethernet Private LAN (EP-LAN)	✓	✓	✓	✓	✓	✓	✓
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✓	✓	✓	✓	✓	✓	✓
Ethernet Virtual Private Tree (EVP-Tree)	✓	✓	✓	✓	✓	✓	✓
Ethernet Virtual Private LAN (EVP-LAN)	✓	✓	✓	✓	✓	✓	✓
Supported Networks (Encryption)							
Ethernet	✓	✓	✓	✓	✓	✓	✓
MPLS (MPLSoE)	✓	✓	✓	✓	✓	✓	✓
MPLS (MPLSoIP)	✓	✓	✓	✓	✓	✓	✓
IPv4	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✓	✓
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✓	✓	✓	✓	✓	✓	✓
MPLS (EoMPLS)	✓	✓	✓	✓	✓	✓	✓
IPv4 (including EoIP and MPLSoIP)	✓	✓	✓	✓	✓	✓	✓
TCP	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓
IPv6 (including EoIP and MPLSoIP)	✓	✓	✓	✓	✓	✓	✓
TCP	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓
Supported Usage Scenarios							
Single tenant	✓	✓	✓	✓	✓	✓	✓
Multi-tenant	✓	✓	✓	✓	✓	✓	✓
per port				✓	✓	✓	(✓)
per port per VLAN	✓	✓	✓	✓	✓	✓	✓
Self-managed	✓	✓	✓	✓	✓	✓	✓
Managed encryption service	✓	✓	✓	✓	✓	✓	✓
Managed security service	✓	✓	✓	✓	✓	✓	✓

Platform

Platform used								
	Mainboard/Firmware	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia
	Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Operating Modes								
	Line Mode	✓	✓	✓	✓	✓	✓	✓
	Multipoint Mode	✓	✓	✓	✓	✓	✓	✓

Data Plane Encryption Standard and Processing

Encryption Standard								
	Block Cipher	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Alternative Mode of Operation							
	Key Length (in bit)	256	256	256	256	256	256	256
Processing Method								
	cut-through	✓	✓	✓	✓	✓	✓	✓
	store&forward	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware								
	FPGA	✓	✓	✓	✓	✓	✓	✓
	ASIC							
	CPU							
Latency								
Latency P2P Mode	cut-through	<42µs	<42µs	<4µs	<8µs	<4µs	<2µs	<2µs
	store & forward	<42µs	<48µs	<4µs	<9µs	<4µs	<2µs	<2µs
Latency MP Mode	cut-through	<42µs	<42µs	<4µs	<8µs	<4µs	<2µs	<2µs
	store & forward	<42µs	<48µs	<4µs	<9µs	<4µs	<2µs	<2µs
Performance Documentation								
Ethernet Throughput & Latency Data available		✓	✓	✓	✓	✓	✓	✓
RFC 2544 Throughput & Latency Data available		✓	✓	✓	✓	✓	✓	✓

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✓	✓	✓	✓	✓	✓	✓
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓
	Frame overhead (authenticated encryption)	20/28	20/28	20/28	20/28	20/28	20/28	20/28
	Ethernet multi-hop support	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Transport (Payload only)		✓	✓	✓	✓	✓	✓	✓
	Max. number of peers	1000	1000	1000	1000	1000	1000	1000
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Definable encryption offset (fixed)	✓	✓	✓	✓	✓	✓	✓
	Variable encryption offset	✓	✓	✓	✓	✓	✓	✓
	Adaptive encryption offset based on frame content	✓	✓	✓	✓	✓	✓	✓
	Registered EtherType	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	20/28	20/28	20/28	20/28	20/28	20/28	20/28
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓
Tunnel (Ethernet over Ethernet)		✓	✓	✓	✓	✓	✓	✓
	Max. number of peers	32	32	32	32	32	32	32
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)		✓	✓	✓	✓	✓	✓	✓
	Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP
	Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓

Native IP Encryption

Supported IP versions								
	IPv4	✓	✓	✓	✓	✓	✓	✓
	IPv6	✓	✓	✓	✓	✓	✓	✓
Supported transmission protocols								
	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
Transport Mode								
	Mximum number of peers	1000	1000	1000	1000	1000	1000	1000
	Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Additional Authenticated Data (header)	✓	✓	✓	✓	✓	✓	✓
	Replay Protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10
	Packet overhead authenticated encryption (AE)	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68
Transport Tunnel Mode								
	Mximum number of peers	1000	1000	1000	1000	1000	1000	1000
	Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Additional Authenticated Data (header)	✓	✓	✓	✓	✓	✓	✓
	Replay Protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10
	Packet overhead authenticated encryption (AE)	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68

Selective Processing (Encryption, Pass, Discard)

Based on MAC Address		✓	✓	✓	✓	✓	✓	✓
Based on VLAN ID		✓	✓	✓	✓	✓	✓	✓
Based on Ethertype		✓	✓	✓	✓	✓	✓	✓
Based on Multicast Group		✓	✓	✓	✓	✓	✓	✓
Based on Presence of MPLS Tag		✓	✓	✓	✓	✓	✓	✓
Based on IP Address		✓	✓	✓	✓	✓	✓	✓
Combination of multiple selection criteria		✓	✓	✓	✓	✓	✓	✓

Mixed Ethernet, MPLS, EoIP and IP Support

Based on VLAN ID								
	MPLS	✓	✓	✓	✓	✓	✓	✓
	EoIP	✓	✓	✓	✓	✓	✓	✓
	IP	✓	✓	✓	✓	✓	✓	✓
Based on presence of MPLS tag								
	MPLS	✓	✓	✓	✓	✓	✓	✓
	EoIP	✓	✓	✓	✓	✓	✓	✓
	IP	✓	✓	✓	✓	✓	✓	✓
Based on VLAN ID and presence of MPLS tag								
	MPLS	✓	✓	✓	✓	✓	✓	✓
	EoIP	✓	✓	✓	✓	✓	✓	✓
	IP	✓	✓	✓	✓	✓	✓	✓

Extended Security Features

AES S-box customization

Costumizable AES S-box	✓	✓	✓	✓	✓	✓	✓

Traffic Masking

Method							
Fixed MTU size	✓	✓	✓	✓	✓	✓	✓
Synthetic traffic injection	✓	✓	✓	✓	✓	✓	✓
Supported topologies							
P2P	✓	✓	✓	✓	✓	✓	✓
P2MP	✓	✓	✓	✓	✓	✓	✓

Control Plane Options and Security

Control Plane Options							
In-band	✓	✓	✓	✓	✓	✓	✓
Out-of-band	✓	✓	✓	✓	✓	✓	✓
Option to separate key exchange from control plane	✓	✓	✓	✓	✓	✓	✓
Protection layer (in-band)							
Ethernet (layer 2)	✓	✓	✓	✓	✓	✓	✓
IP (layer 3)	✓	✓	✓	✓	✓	✓	✓
Transport (layer 4)	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware (in-band)							
FPGA	✓	✓	✓	✓	✓	✓	✓
ASIC							
CPU	✓	✓	✓	✓	✓	✓	✓
Encryption (in-band)							
Separate from data plane encryption	✓	✓	✓	✓	✓	✓	✓
Same protection level as data plane encyption	✓	✓	✓	✓	✓	✓	✓
DoS Resiliency (in-band)							
line rate	✓	✓	✓	✓	✓	✓	✓

Auto-discovery

Auto-discovery of network encryptors	✓	✓	✓	✓	✓	✓	✓
Auto-discovery of key servers	✓	✓	✓	✓	✓	✓	✓
Auto-discovery of VLANs	✓	✓	✓	✓	✓	✓	✓
Disabling of auto-discovery	✓	✓	✓	✓	✓	✓	✓

Key Server

Integrated Key Server	✓	✓	✓	✓	✓	✓	✓
Support for external Key Server	✓	✓	✓	✓	✓	✓	✓
External Key Server							
Support for multiple distributed Key Servers	✓	✓	✓	✓	✓	✓	✓
Support for fail-over to back-up Key Server	✓	✓	✓	✓	✓	✓	✓
Number of backup key servers	16	16	16	16	16	16	16
Number of hierarchy levels of backup key servers	16	16	16	16	16	16	16
Autonomous operation	✓	✓	✓	✓	✓	✓	✓

Key Management

Key Generation and Storage							
Hardware Random Number Generation	✓	✓	✓	✓	✓	✓	✓
Tamper Security Key Storage (tamper-evident or tamper-proof)	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
Elliptic Curve Cryptography (ECC)							
Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Key strength (in bit)	256	256	256	256	256	256	256
Supported Curves:							
NIST	✓	✓	✓	✓	✓	✓	✓
Brainpool	✓	✓	✓	✓	✓	✓	✓
Custom Curves	✓	✓	✓	✓	✓	✓	✓

Hash Algorithms								
SHA-2	Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Key strenght (Image/Collision Resistance)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CBC-MAC-GCM								
	Key length	256	256	256	256	256	256	256
	Key strength	256	256	256	256	256	256	256
Device Authentication								
Symmetric Signature: Pre-shared Key (PSK)		✓	✓	✓	✓	✓	✓	✓
	Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
	Key length	256	256	256	256	256	256	256
	Key strenght (in bit)	256	256	256	256	256	256	256
Asymmetric Signature: Certificate		optional	optional	optional	optional	optional	optional	optional
	Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
	Key lenght	512	512	512	512	512	512	512
	Key strenght (in bit)	256	256	256	256	256	256	256
Ad-hoc authentication of peers (manual)		✓	✓	✓	✓	✓	✓	✓
Signature key protocol		AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****
Key Agreement and Key Exchange								
Master Key (KEK) Agreement		ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key		✓	✓	✓	✓	✓	✓	✓
Minimum suggested Time Interval for Master Key Change (min)		60	60	60	60	60	60	60
Separate Master Key (KEK) per site		✓	✓	✓	✓	✓	✓	✓
Separate Master Key (KEK) per group		✓	✓	✓	✓	✓	✓	✓
Session Key (DEK) Exchange Agreement		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys		✓	✓	✓	✓	✓	✓	✓
Minimum Time Interval for Session Key Change (min)		1	1	1	1	1	1	1
Key Exchange Options								
In-band		✓	✓	✓	✓	✓	✓	✓
Out-of-band		✓	✓	✓	✓	✓	✓	✓
Key exchange via raw Ethernet		✓	✓	✓	✓	✓	✓	✓
In-band key exchange via IP	IPv4	✓	✓	✓	✓	✓	✓	✓
	IPv6	✓	✓	✓	✓	✓	✓	✓
Quantum-safe Key Exchange		✓	✓	✓	✓	✓	✓	✓
	Symmetric Encryption of Asymmetric Key Exchange	✓	✓	✓	✓	✓	✓	✓
	QKD (optical short range only)							
	Quantum-safe Key Exchange Algorithm	Frodo optional	Frodo optional	Frodo optional	Frodo optional	Frodo optional	Frodo optional	Frodo optional
Key System								
Point-to-Point Key System								
Supported key system								
	Pairwise	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:								
	MAC Address	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓
	Group	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
Point-to-Multipoint Key System								
Supported key systems:								
	Pairwise	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:								
	MAC Address	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓
	Group	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓

Multipoint Key System								
Supported key systems:								
	Pairwise	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
	Mixed (pairwise unicast, group multicast)	✓	✓	✓	✓	✓	✓	✓
Key assignment based on:								
	MAC address (pairwise and mixed)	✓	✓	✓	✓	✓	✓	✓
	Multicast groups (mixed)	✓	✓	✓	✓	✓	✓	✓
	VLAN ID (group)	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓
	Group (group)	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
	IP Multicast Group	✓	✓	✓	✓	✓	✓	✓
Individual key per multicast group		✓	✓	✓	✓	✓	✓	✓
Individual key per broadcast group (VLAN ID)		✓	✓	✓	✓	✓	✓	✓
Group Key System Specifics								
Additional separate authentication per group		✓	✓	✓	✓	✓	✓	✓
Group Membership Definition								
	Multicast group membership	✓	✓	✓	✓	✓	✓	✓
	Individual membership	✓	✓	✓	✓	✓	✓	✓
	Network membership	✓	✓	✓	✓	✓	✓	✓
	VLAN membership	✓	✓	✓	✓	✓	✓	✓
	Trunked VLAN membership	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
Exclusion								
	MAC address	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓
	Frames with MPLS tag	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
	IP Muticast Group	✓	✓	✓	✓	✓	✓	✓
Group Key Distribution								
	Unicast (unique KEK per group member)	✓	✓	✓	✓	✓	✓	✓
	Broadcast (same KEK for all group members)	✓	✓	✓	✓	✓	✓	✓
Network Support								
Bump in the Wire deployment		✓	✓	✓	✓	✓	✓	✓
Jumbo Frame Support		✓	✓	✓	✓	✓	✓	✓
Ethernet Flow Control via PAUSE		✓	✓	✓	✓	✓	✓	✓
Tagging of untagged frames		✓	✓	✓	✓	✓	✓	✓
Ethernet Fragmentation/Defragmentation		✓	✓	✓	✓	✓	✓	✓
	Point-to-Point	✓	✓	✓	✓	✓	✓	✓
	Point-to-Multipoint	✓	✓	✓	✓	✓	✓	✓
	Multipoint	✓	✓	✓	✓	✓	✓	✓
Dead Peer Detection		✓	✓	✓	✓	✓	✓	✓
Optical Loss Pass-Through		N/A	N/A	✓	✓	✓	✓	✓
Link Loss Carry Forward		✓	✓	N/A	N/A	N/A	N/A	N/A
System Configuration and Management Access								
IPv4		✓	✓	✓	✓	✓	✓	✓
IPv6		✓	✓	✓	✓	✓	✓	✓
Out-of-band Management		✓	✓	✓	✓	✓	✓	✓
	RS-232/V.24	✓	✓	✓	✓	✓	✓	✓
	Separate Ethernet port	✓	✓	✓	✓	✓	✓	✓
Smart Card (Secure Card) Support		✓	✓	✓	✓	✓	✓	✓
USB Port								✓
In-band Management		✓	✓	✓	✓	✓	✓	✓
	SSH	✓	✓	✓	✓	✓	✓	✓
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only	read-only
	TLS							
	Proprietary	✓	✓	✓	✓	✓	✓	✓
Remote Monitoring (SNMP)		v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3

Logs

Event Log (local)	✓	✓	✓	✓	✓	✓	✓
Audit Log (local)	✓	✓	✓	✓	✓	✓	✓
Syslog Support (Server)	✓	✓	✓	✓	✓	✓	✓

Unit

Height in 19" Rack	1U	1U	1U	1U	1U	1U	1U
Number of external encrypted Ethernet ports	1	1	1	1-4	1-4	1-4	1
Physical Device Access	back	front	front	front	front	front	front
Redundant Power Supply	✓	✓	✓	✓	✓	✓	✓
Redundant, hot-swappable power supply			✓	✓	✓	✓	✓
High Availability functionality (two-node cluster)	1:1	1:1	1:1	1:1	1:1	1:1	1:1
MTBF	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals			BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL)				
Safety Approvals			EN55032 Class B, FCC Part 15 Class B, ROHS				
Boot Time							
Cold boot until operational (P2P)	25s	25s	25s	25s	25s	25s	25s
Warm boot until operational (P2P)	27s	27s	27s	27s	27s	27s	27s

Management Software

User Interface	Native PC application (applets)	✓	✓	✓	✓	✓	✓	✓
	Embedded Webapp							
	CLI	✓	✓	✓	✓	✓	✓	✓
Initial Device Set-up								
	Local (out-of-band)	✓	✓	✓	✓	✓	✓	✓
	Remote (out-of-band)	✓	✓	✓	✓	✓	✓	✓
Device Configuration								
	Local (out-of-band)	✓	✓	✓	✓	✓	✓	✓
	Remote (in-band)	✓	✓	✓	✓	✓	✓	✓
	Remote (out-of-band)	✓	✓	✓	✓	✓	✓	✓
Management Access								
	Role-based access	✓	✓	✓	✓	✓	✓	✓
	Identity-based authentication of user	✓	✓	✓	✓	✓	✓	✓
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	5	5	5	5	5	5	5
	Strict internal separation of users	✓	✓	✓	✓	✓	✓	✓
Device Management								
	Device Diagnostics	✓	✓	✓	✓	✓	✓	✓
	Link Monitoring (SNMP)	✓	✓	✓	✓	✓	✓	✓
	Connection Diagnostics	✓	✓	✓	✓	✓	✓	✓
	In-band Network Diagnostics	✓	✓	✓	✓	✓	✓	✓
	Remote Update/Upgrade	✓	✓	✓	✓	✓	✓	✓
Certificate Authority & Management		optional	optional	optional	optional	optional	optional	optional
	Certificate Creation	optional	optional	optional	optional	optional	optional	optional
	Certificate Management	optional	optional	optional	optional	optional	optional	optional
Key Management								
	Group creation	✓	✓	✓	✓	✓	✓	✓
	Group isolation	✓	✓	✓	✓	✓	✓	✓
	Key assignment	✓	✓	✓	✓	✓	✓	✓
	Fail-over configuration	✓	✓	✓	✓	✓	✓	✓

Price

List Price Encryption Unit (in €)	on request	on request	on request	on request	on request	on request	on request
Per extermal Key Server (in €); optional, no requirement	on request	on request	on request	on request	on request	on request	on request
Required Management Software (SINA Management Software optional)							
2-10 encryptors	included	included	included	included	included	included	included
11-25 encryptors	included	included	included	included	included	included	included
26-50 encryptors	included	included	included	included	included	included	included
51+ encryptors	included	included	included	included	included	included	included
Warranty Period (months)	36-60	36-60	36-60	36-60	36-60	36-60	36-60
Warranty Coverage Parts & Work	✓	✓	✓	✓	✓	✓	✓
Basic Support (9 to 5, e-mail, phone)	✓	✓	✓	✓	✓	✓	✓
Software updates and upgrades	✓	✓	✓	✓	✓	✓	✓
Warranty Extension (per year)	on request	on request	on request	on request	on request	on request	on request

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

Securosys

	Centurion 50/100 compact	Centurion 1G compact	Centurion 1G	Centurion 10G	Centurion 4x10G	Centurion 40G	Centurion 100G
Line Interface/Supported Line Rates							
10 Mbs	✓/RJ45	✓/RJ45					
100 Mbs	✓/RJ45	✓/RJ45 (/SFP on request)					
1 Gbps	✓/RJ45	✓/RJ45 (/SFP on request)	✓/SFP+	✓4x /SFP			
4 x 1 Gbps				✓4x /SFP			
10 Gbps			✓/SFP+		✓4x /SFP+	✓/QSFP+/SFP+	
25 Gps							✓/QSFP28
4 x 10 Gbps					✓4x /SFP+	✓/QSFP+	
40 Gbps						✓/QSFP+	✓/QSFP28
50 Gbps							✓/QSFP28
100 Gbps							✓/QSFP28/FEC
Virtual Appliance							
Supported Network Topologies (single-port)							
Point-to-Point (P2P)	✓	✓	✓	✓	✓	✓	✓
Point-to-Multipoint (P2MP)	✓	✓	✓	✓	✓	✓	✓
Multipoint (MP)	✓	✓	✓	✓	✓	✓	✓
Supported Network Topologies (multi-port/per port)							
Point-to-Point (P2P)				✓	✓	✓	✓
Point-to-Multipoint (P2MP)				✓	✓	✓	✓
Multipoint (MP)				✓	✓	✓	✓
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)	✓	✓	✓	✓	✓	✓	✓
Ethernet Private Tree (EP-Tree)	✓	✓	✓	✓	✓	✓	✓
Ethernet Private LAN (EP-LAN)	✓	✓	✓	✓	✓	✓	✓
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)	✓	✓	✓	✓	✓	✓	✓
Ethernet Virtual Private Tree (EVP-Tree)	✓	✓	✓	✓	✓	✓	✓
Ethernet Virtual Private LAN (EVP-LAN)	✓	✓	✓	✓	✓	✓	✓
Supported Networks (Encryption)							
Ethernet	✓	✓	✓	✓	✓	✓	✓
MPLS (MPLSoE)	✓	✓	✓	✓	✓	✓	✓
MPLS (MPLSoIP)	✓	✓	✓	✓	✓	✓	✓
IPv4	✓	✓	✓	✓	✓	✓	✓
IPv6	✓	✓	✓	✓	✓	✓	✓
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✓	✓	✓	✓	✓	✓	✓
MPLS (EoMPLS)	✓	✓	✓	✓	✓	✓	✓
IPv4 (including EoIP and MPLSoIP)	✓	✓	✓	✓	✓	✓	✓
TCP	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓
IPv6 (including EoIP and MPLSoIP)	✓	✓	✓	✓	✓	✓	✓
TCP	✓	✓	✓	✓	✓	✓	✓
UDP	✓	✓	✓	✓	✓	✓	✓
Supported Usage Scenarios							
Single tenant	✓	✓	✓	✓	✓	✓	✓
Multi-tenant	✓	✓	✓	✓	✓	✓	✓
per port				✓	✓	✓	✓
per port per VLAN	✓	✓	✓	✓	✓	✓	✓
Self-managed	✓	✓	✓	✓	✓	✓	✓
Managed encryption service	✓	✓	✓	✓	✓	✓	✓
Managed security service	✓	✓	✓	✓	✓	✓	✓

Platform

Platform used								
	Mainboard/Firmware	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia
	Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Operating Modes								
	Line Mode	✓	✓	✓	✓	✓	✓	✓
	Multipoint Mode	✓	✓	✓	✓	✓	✓	✓

Data Plane Encryption Standard and Processing

Encryption Standard								
	Block Cipher	AES	AES	AES	AES	AES	AES	AES
	Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Alternative Mode of Operation							
	Key Length (in bit)	256	256	256	256	256	256	256
Processing Method								
	cut-through	✓	✓	✓	✓	✓	✓	✓
	store&forward	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware								
	FPGA	✓	✓	✓	✓	✓	✓	✓
	ASIC							
	CPU							
Latency								
Latency P2P Mode	cut-through	<42µs	<42µs	<4µs	<8µs	<4µs	<2µs	<2µs
	store & forward	<42µs	<48µs	<4µs	<9µs	<4µs	<2µs	<2µs
Latency MP Mode	cut-through	<42µs	<42µs	<4µs	<8µs	<4µs	<2µs	<2µs
	store & forward	<42µs	<48µs	<4µs	<9µs	<4µs	<2µs	<2µs
Performance Documentation								
	Ethernet Throughput & Latency Data available	✓	✓	✓	✓	✓	✓	✓
	RFC 2544 Throughput & Latency Data available	✓	✓	✓	✓	✓	✓	✓

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)		✓	✓	✓	✓	✓	✓	✓
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓
	Frame overhead (authenticated encryption)	20/28	20/28	20/28	20/28	20/28	20/28	20/28
	Ethernet multi-hop support	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Transport (Payload only)		✓	✓	✓	✓	✓	✓	✓
	Max. number of peers	1000	1000	1000	1000	1000	1000	1000
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Definable encryption offset (fixed)	✓	✓	✓	✓	✓	✓	✓
	Variable encryption offset	✓	✓	✓	✓	✓	✓	✓
	Adaptive encryption offset based on frame content	✓	✓	✓	✓	✓	✓	✓
	Registered EtherType	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	20/28	20/28	20/28	20/28	20/28	20/28	20/28
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓
Tunnel (Ethernet over Ethernet)		✓	✓	✓	✓	✓	✓	✓
	Max. number of peers	32	32	32	32	32	32	32
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*	32/40*
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)		✓	✓	✓	✓	✓	✓	✓
	Supported transmission protocols (UDP/TCP)	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP	native IP/UDP
	Max. number of peers	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)	2 (P2P), 1000 (MP)
	Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	AAD (additional authenticated data)	✓	✓	✓	✓	✓	✓	✓
	Replay protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Registered Ethertype	✓	✓	✓	✓	✓	✓	✓
	Counter length (in bytes)	10	10	10	10	10	10	10
	Frame overhead authenticated encryption (AE)	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*	54/62*
	Ethernet multi-hop support	✓	✓	✓	✓	✓	✓	✓

Native IP Encryption

Supported IP versions								
	IPv4	✓	✓	✓	✓	✓	✓	✓
	IPv6	✓	✓	✓	✓	✓	✓	✓
Supported transmission protocols								
	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
Transport Mode								
	Mximum number of peers	1000	1000	1000	1000	1000	1000	1000
	Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Additional Authenticated Data (header)	✓	✓	✓	✓	✓	✓	✓
	Replay Protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10
	Packet overhead authenticated encryption (AE)	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68
Transport Tunnel Mode								
	Mximum number of peers	1000	1000	1000	1000	1000	1000	1000
	Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM	GCM
	Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16	8/16
	Additional Authenticated Data (header)	✓	✓	✓	✓	✓	✓	✓
	Replay Protection	✓	✓	✓	✓	✓	✓	✓
	Variable replay window (size)	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s	✓ 0-30s
	Counter length (in bytes)	10	10	10	10	10	10	10
	Packet overhead authenticated encryption (AE)	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68	IPv4: 40/48 IPv6: 60/68	IPv4: 40/48 IPv6:60/68

Selective Processing (Encryption, Pass, Discard)

Based on MAC Address	✓	✓	✓	✓	✓	✓	✓
Based on VLAN ID	✓	✓	✓	✓	✓	✓	✓
Based on Ethertype	✓	✓	✓	✓	✓	✓	✓
Based on Multicast Group	✓	✓	✓	✓	✓	✓	✓
Based on Presence of MPLS Tag	✓	✓	✓	✓	✓	✓	✓
Based on IP Address	✓	✓	✓	✓	✓	✓	✓
Combination of multiple selection criteria	✓	✓	✓	✓	✓	✓	✓

Mixed Ethernet, MPLS, EoIP and IP Support

Based on VLAN ID							
	MPLS	✓	✓	✓	✓	✓	✓	✓
	EoIP	✓	✓	✓	✓	✓	✓	✓
	IP	✓	✓	✓	✓	✓	✓	✓
Based on presence of MPLS tag								
	MPLS	✓	✓	✓	✓	✓	✓	✓
	EoIP	✓	✓	✓	✓	✓	✓	✓
	IP	✓	✓	✓	✓	✓	✓	✓
Based on VLAN ID and presence of MPLS tag								
	MPLS	✓	✓	✓	✓	✓	✓	✓
	EoIP	✓	✓	✓	✓	✓	✓	✓
	IP	✓	✓	✓	✓	✓	✓	✓

Extended Security Features

AES S-box customization

Costumizable AES S-box		✓	✓	✓	✓	✓	✓	✓

Traffic Masking

Method								
	Fixed MTU size	✓	✓	✓	✓	✓	✓	✓
	Synthetic traffic injection	✓	✓	✓	✓	✓	✓	✓
Supported topologies								
	P2P	✓	✓	✓	✓	✓	✓	✓
	P2MP	✓	✓	✓	✓	✓	✓	✓

Control Plane Options and Security

Control Plane Options								
	In-band	✓	✓	✓	✓	✓	✓	✓
	Out-of-band	✓	✓	✓	✓	✓	✓	✓
	Option to separate key exchange from control plane	✓	✓	✓	✓	✓	✓	✓
Protection layer (in-band)								
	Ethernet (layer 2)	✓	✓	✓	✓	✓	✓	✓
	IP (layer 3)	✓	✓	✓	✓	✓	✓	✓
	Transport (layer 4)	✓	✓	✓	✓	✓	✓	✓
Encryption Hardware (in-band)								
	FPGA	✓	✓	✓	✓	✓	✓	✓
	ASIC							
	CPU	✓	✓	✓	✓	✓	✓	✓
Encryption (in-band)								
	Separate from data plane encryption	✓	✓	✓	✓	✓	✓	✓
	Same protection level as data plane encyption	✓	✓	✓	✓	✓	✓	✓
DoS Resiliency (in-band)								
	line rate	✓	✓	✓	✓	✓	✓	✓

Auto-discovery

Auto-discovery of network encryptors		✓	✓	✓	✓	✓	✓	✓
Auto-discovery of key servers		✓	✓	✓	✓	✓	✓	✓
Auto-discovery of VLANs		✓	✓	✓	✓	✓	✓	✓
Disabling of auto-discovery		✓	✓	✓	✓	✓	✓	✓

Key Server

Integrated Key Server		✓	✓	✓	✓	✓	✓	✓
Support for external Key Server		✓	✓	✓	✓	✓	✓	✓
External Key Server								
Support for multiple distributed Key Servers		✓	✓	✓	✓	✓	✓	✓
Support for fail-over to back-up Key Server		✓	✓	✓	✓	✓	✓	✓
	Number of backup key servers	16	16	16	16	16	16	16
	Number of hierarchy levels of backup key servers	16	16	16	16	16	16	16
Autonomous operation		✓	✓	✓	✓	✓	✓	✓

Key Management

Key Generation and Storage								
Hardware Random Number Generation		✓	✓	✓	✓	✓	✓	✓
Tamper Security Key Storage (tamper-evident or tamper-proof)		TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)								
Elliptic Curve Cryptography (ECC)								
	Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521
	Key strength (in bit)	256	256	256	256	256	256	256
Supported Curves:								
	NIST	✓	✓	✓	✓	✓	✓	✓
	Brainpool	✓	✓	✓	✓	✓	✓	✓
	Custom Curves	✓	✓	✓	✓	✓	✓	✓

Hash Algorithms								
SHA-2	Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Key strenght (Image/Collision Resistance)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CBC-MAC-GCM								
	Key length	256	256	256	256	256	256	256
	Key strength	256	256	256	256	256	256	256
Device Authentication								
Symmetric Signature: Pre-shared Key (PSK)		✓	✓	✓	✓	✓	✓	✓
	Maximum number of PSKs per encryptor	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)	512 (recommended:18)
	Key length	256	256	256	256	256	256	256
	Key strenght (in bit)	256	256	256	256	256	256	256
Asymmetric Signature: Certificate		optional	optional	optional	optional	optional	optional	optional
	Maximum number of certificates per encryptor	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)	64 (recommended:18)
	Key lenght	512	512	512	512	512	512	512
	Key strenght (in bit)	256	256	256	256	256	256	256
Ad-hoc authentication of peers (manual)		✓	✓	✓	✓	✓	✓	✓
Signature key protocol		AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****	AES-MAC/ECDSA****
Key Agreement and Key Exchange								
Master Key (KEK) Agreement		ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Master Key		✓	✓	✓	✓	✓	✓	✓
Minimum suggested Time Interval for Master Key Change (min)		60	60	60	60	60	60	60
Separate Master Key (KEK) per site		✓	✓	✓	✓	✓	✓	✓
Separate Master Key (KEK) per group		✓	✓	✓	✓	✓	✓	✓
Session Key (DEK) Exchange Agreement		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol		atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Automatic Change of Session Keys		✓	✓	✓	✓	✓	✓	✓
Minimum Time Interval for Session Key Change (min)		1	1	1	1	1	1	1
Key Exchange Options								
In-band		✓	✓	✓	✓	✓	✓	✓
Out-of-band		✓	✓	✓	✓	✓	✓	✓
Key exchange via raw Ethernet		✓	✓	✓	✓	✓	✓	✓
In-band key exchange via IP	IPv4	✓	✓	✓	✓	✓	✓	✓
	IPv6	✓	✓	✓	✓	✓	✓	✓
Quantum-safe Key Exchange		✓	✓	✓	✓	✓	✓	✓
	Symmetric Encryption of Asymmetric Key Exchange	✓	✓	✓	✓	✓	✓	✓
	QKD (optical short range only)							
	Quantum-safe Key Exchange Algorithm	Frodo optional	Frodo optional	Frodo optional	Frodo optional	Frodo optional	Frodo optional	Frodo optional
Key System								
Point-to-Point Key System								
Supported key system								
	Pairwise	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:								
	MAC Address	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓
	Group	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
Point-to-Multipoint Key System								
Supported key systems:								
	Pairwise	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
Key assignment based on:								
	MAC Address	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓
	Group	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓

Multipoint Key System								
Supported key systems:								
	Pairwise	✓	✓	✓	✓	✓	✓	✓
	Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group	Bidirectional Group
	Mixed (pairwise unicast, group multicast)	✓	✓	✓	✓	✓	✓	✓
Key assignment based on:								
	MAC address (pairwise and mixed)	✓	✓	✓	✓	✓	✓	✓
	Multicast groups (mixed)	✓	✓	✓	✓	✓	✓	✓
	VLAN ID (group)	✓	✓	✓	✓	✓	✓	✓
	Port	✓	✓	✓	✓	✓	✓	✓
	Group (group)	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
	IP Multicast Group	✓	✓	✓	✓	✓	✓	✓
Individual key per multicast group		✓	✓	✓	✓	✓	✓	✓
Individual key per broadcast group (VLAN ID)		✓	✓	✓	✓	✓	✓	✓
Group Key System Specifics								
Additional separate authentication per group		✓	✓	✓	✓	✓	✓	✓
Group Membership Definition								
	Multicast group membership	✓	✓	✓	✓	✓	✓	✓
	Individual membership	✓	✓	✓	✓	✓	✓	✓
	Network membership	✓	✓	✓	✓	✓	✓	✓
	VLAN membership	✓	✓	✓	✓	✓	✓	✓
	Trunked VLAN membership	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
Exclusion								
	MAC address	✓	✓	✓	✓	✓	✓	✓
	VLAN ID	✓	✓	✓	✓	✓	✓	✓
	Frames with MPLS tag	✓	✓	✓	✓	✓	✓	✓
	IP Address	✓	✓	✓	✓	✓	✓	✓
	IP Muticast Group	✓	✓	✓	✓	✓	✓	✓
Group Key Distribution								
	Unicast (unique KEK per group member)	✓	✓	✓	✓	✓	✓	✓
	Broadcast (same KEK for all group members)	✓	✓	✓	✓	✓	✓	✓
Network Support								
Bump in the Wire deployment		✓	✓	✓	✓	✓	✓	✓
Jumbo Frame Support		✓	✓	✓	✓	✓	✓	✓
Ethernet Flow Control via PAUSE		✓	✓	✓	✓	✓	✓	✓
Tagging of untagged frames		✓	✓	✓	✓	✓	✓	✓
Ethernet Fragmentation/Defragmentation		✓	✓	✓	✓	✓	✓	✓
	Point-to-Point	✓	✓	✓	✓	✓	✓	✓
	Point-to-Multipoint	✓	✓	✓	✓	✓	✓	✓
	Multipoint	✓	✓	✓	✓	✓	✓	✓
Dead Peer Detection		✓	✓	✓	✓	✓	✓	✓
Optical Loss Pass-Through		N/A	N/A	✓	✓	✓	✓	✓
Link Loss Carry Forward		✓	✓	N/A	N/A	N/A	N/A	N/A
System Configuration and Management Access								
IPv4		✓	✓	✓	✓	✓	✓	✓
IPv6		✓	✓	✓	✓	✓	✓	✓
Out-of-band Management		✓	✓	✓	✓	✓	✓	✓
	RS-232/V.24	✓	✓	✓	✓	✓	✓	✓
	Separate Ethernet port	✓	✓	✓	✓	✓	✓	✓
Smart Card (Secure Card) Support		✓	✓	✓	✓	✓	✓	✓
USB Port								✓
In-band Management		✓	✓	✓	✓	✓	✓	✓
	SSH	✓	✓	✓	✓	✓	✓	✓
	SNMP (read-only/read-write)	read-only	read-only	read-only	read-only	read-only	read-only	read-only
	TLS							
	Proprietary	✓	✓	✓	✓	✓	✓	✓
Remote Monitoring (SNMP)		v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3	v2c/v3

Logs

Event Log (local)		✓	✓	✓	✓	✓	✓	✓
Audit Log (local)		✓	✓	✓	✓	✓	✓	✓
Syslog Support (Server)		✓	✓	✓	✓	✓	✓	✓

Unit

Height in 19" Rack		1U	1U	1U	1U	1U	1U	1U
Number of external encrypted Ethernet ports		1	1	1	1-4	1-4	1-4	1
Physical Device Access		back	front	front	front	front	front	front
Redundant Power Supply		✓	✓	✓	✓	✓	✓	✓
Redundant, hot-swappable power supply				✓	✓	✓	✓	✓
High Availability functionality (two-node cluster)		1:1	1:1	1:1	1:1	1:1	1:1	1:1
MTBF		> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h	> 50.000h
Tamper Security		TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals		Atmedia platform approved BSI NfD, EU Restrint, NATO Restrint. Apporvals are not inherited.						
Safety Approvals		EN55032 Class B, FCC Part 15 Class B, ROHS						
Boot Time								
	Cold boot until operational (P2P)	25s	25s	25s	25s	25s	25s	25s
	Warm boot until operational (P2P)	27s	27s	27s	27s	27s	27s	27s

Management Software

User Interface	Native PC application (applets)	✓	✓	✓	✓	✓	✓	✓
	Embedded Webapp							
	CLI	✓	✓	✓	✓	✓	✓	✓
Initial Device Set-up								
	Local (out-of-band)	✓	✓	✓	✓	✓	✓	✓
	Remote (out-of-band)	✓	✓	✓	✓	✓	✓	✓
Device Configuration								
	Local (out-of-band)	✓	✓	✓	✓	✓	✓	✓
	Remote (in-band)	✓	✓	✓	✓	✓	✓	✓
	Remote (out-of-band)	✓	✓	✓	✓	✓	✓	✓
Management Access								
	Role-based access	✓	✓	✓	✓	✓	✓	✓
	Identity-based authentication of user	✓	✓	✓	✓	✓	✓	✓
	Number of hierarchy levels	2	2	2	2	2	2	2
	Number of roles	5	5	5	5	5	5	5
	Strict internal separation of users	✓	✓	✓	✓	✓	✓	✓
Device Management								
	Device Diagnostics	✓	✓	✓	✓	✓	✓	✓
	Link Monitoring (SNMP)	✓	✓	✓	✓	✓	✓	✓
	Connection Diagnostics	✓	✓	✓	✓	✓	✓	✓
	In-band Network Diagnostics	✓	✓	✓	✓	✓	✓	✓
	Remote Update/Upgrade	✓	✓	✓	✓	✓	✓	✓
Certificate Authority & Management		optional	optional	optional	optional	optional	optional	optional
	Certificate Creation	optional	optional	optional	optional	optional	optional	optional
	Certificate Management	optional	optional	optional	optional	optional	optional	optional
Key Management								
	Group creation	✓	✓	✓	✓	✓	✓	✓
	Group isolation	✓	✓	✓	✓	✓	✓	✓
	Key assignment	✓	✓	✓	✓	✓	✓	✓
	Fail-over configuration	✓	✓	✓	✓	✓	✓	✓

Price

List Price Encryption Unit (in €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement		on request	on request	on request	on request	on request	on request	on request
Required Management Software								
	2-10 encryptors	included	included	included	included	included	included	included
	11-25 encryptors	included	included	included	included	included	included	included
	26-50 encryptors	included	included	included	included	included	included	included
	51+ encryptors	included	included	included	included	included	included	included
Warranty Period (months)		24	24	24	24	24	24	24
Warranty Coverage	Parts & Work	✓	✓	✓	✓	✓	✓	✓
	Basic Support (9 to 5, e-mail, phone)	✓	✓	✓	✓	✓	✓	✓
	Software updates and upgrades	✓	✓	✓	✓	✓	✓	✓
Warranty Extension (per year)		on request	on request	on request	on request	on request	on request	on request

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

Senetas

	CV1000	CN4010	CN4020	CN6010	CN6100	CN6140	CN9120
Line Interface/Supported Line Rates							
10 Mbs							
100 Mps							
1 Gbps							
4x1 Gbps							
10 Gbps							
4x10 Gbps							
25Gps							
40 Gbps							
100 Gbps							
Virtual Appliance							
Supported Network Topologies							
Point-to-Point (P2P)							
Point-to-Multipoint (P2MP)							
Multipoint (MP)							
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)							
Ethernet Private Tree (EP-Tree)							
Ethernet Private LAN (EP-LAN)							
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)							
Ethernet Virtual Private Tree (EVP-Tree)							
Ethernet Virtual Private LAN (EVP-LAN)							
Supported Networks (Encryption)							
Ethernet							
MPLS (MPLSoE)							
MPLS (MPLSoIP)							
IPv4							
IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)							
MPLS (EoMPLS)							
IPv4 (including EoIP and MPLSoIP)							
TCP							
UDP							
IPv6 (including EoIP and MPLSoIP)							
TCP							
UDP							
Supported Usage Scenarios							
Single tenant							
Multi-tenant							
per-port							
per-VLAN							
Self-managed							
Managed encryption service							
Managed security service							

Platform

Platform used

- Mainboard/Firmware
- Key Management

Operating Modes

- P2P Mode
- Multipoint Mode

Data Plane Encryption Standard and Processing

Encryption Standard

- Block Cipher
- Preferred Mode of Operation
- Alternative Mode of Operation
- Key Length (in bit)

Processing Method

- cut-through
- store&forward

Encryption Hardware

- FPGA
- ASIC
- CPU

Latency

- Latency P2P Mode
  - cut-through
  - store & forward
- Latency MP Mode
  - cut-through
  - store & forward

Performance Documentation

- Ethernet Throughput & Latency Data available
- RFC 2544 Throughput & Latency Data available

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)

- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Counter length (in bytes)
- Registered Ethertype
- Frame overhead (unauthenticated encryption)
- Frame overhead (authenticated encryption)
- Ethernet multi-hop support

Transport (Payload only)

- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Definable encryption offset (fixed)
- Variable encryption offset
- Adaptive encryption offset based on frame content
- Registered EtherType
- Counter length (in bytes)
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Tunnel (Ethernet over Ethernet)

- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Registered Ethertype
- Counter length (in bytes)
- Frame overhead unauthenticated encryption
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)

- Supported transmission protocols (UDP/TCP)
- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Proprietary Ethertype
- Counter length (in bytes)
- Frame overhead unauthenticated encryption
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Native IP Encryption

Supported IP versions

- IPv4
- IPv6

Supported transmission protocols

- TCP
- UDP

Transport Mode

- Mximum number of peers
- Maximum number of IP addresses
- Maximum number of multicast groups
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - Additional Authenticated Data (header)
- Replay Protection
  - Variable replay window (size)
- Counter length (in bytes)
- Packet overhead authenticated encryption (AE)

Transport Tunnel Mode

- Maximum number of peers
- Maximum number of IP addresses
- Maximum number of multicast groups
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - Additional Authenticated Data (header)
- Replay Protection
  - Variable replay window (size)
- Counter length (in bytes)
- Packet overhead authenticated encryption (AE)

Selective Encryption

- Based on MAC Address
- Based on VLAN ID
- Based on Ethertype
- Based on Multicast Group
- Based on Presence of MPLS Tag
- Based on IP Address
- Combination of multiple selection criteria

Mixed Ethernet, MPLS, EoIP and IP Support

Based on VLAN ID

- MPLS
- EoIP
- IP

Based on presence of MPLS tag

- MPLS
- EoIP
- IP

Based on VLAN ID and presence of MPLS tag

- MPLS
- EoIP
- IP

Extended Security Features

Customizable AES S-Box

AES S-Box Customization

Traffic Masking

Traffic Flow Security

P2P
P2MP

Method

Configurable uniform frame size
Synthetic traffic injection

Control Plane

Control Plane Options

In-band
Out-of-band
Option to separate key exchange from control plane

Protection layer (in-band)

Ethernet (layer 2)
IP (layer 3)
Transport (layer 4)

Encryption Hardware (in-band)

FPGA
ASIC
CPU

Encryption (in-band)

Separate from data plane encryption
Same protection level as data plane encyption

DoS Resiliency (in-band)

line rate

Auto-discovery

Auto-discovery of network encryptors
Auto-discovery of key servers
Auto-discovery of VLANs
Disabling of auto-discovery

Key Server

Integrated Key Server
Support for external Key Server
External Key Server
Support for multiple distributed Key Servers
Support for fail-over to back-up Key Server

Autonomous operation

Key Management

Key Generation and Storage

Hardware Random Number Generation
Tamper Security Key Storage (tamper-evident or tamper-proof)

Asymmetric Key Algorithms (Public Key Cryptography)

RSA

Key length
Key strength (in bit)

Elliptic Curve Cryptography (ECC)

Key length
Key strength (in bit)

Supported Curves:

NIST
Brainpool
Custom Curves

Hash Algorithms

SHA-2
- Key length
- Key strenght (Image/Collision Resistance)

Device Authentication

Symmetric Signature: Pre-shared Key (PSK)
- Maximum number of PSKs per encryptor
- Key length
- Key strenght (in bit)

Asymmetric Signature: Certificate
- Maximum number of certificates per encryptor
- Key length
- Key strength (in bit)

Ad-hoc authentication of peers (manual)
Signature key protocol

Key Agreement and Key Exchange

Master Key (KEK) Agreement
Master Key (KEK) Exchange Protocol
Automatic Change of Master Key
Minimum suggested Time Interval for Master Key Change (min)
Separate Master Key (KEK) per site
Separate Master Key (KEK) per group

Session Key (DEK) Exchange Agreement
Session Key (DEK) Exchange Protocol
Automatic Change of Session Keys
Minimum Time Interval for Session Key Change (min)

Quantum-safe Key Exchange

Symmetric Encryption of Asymmetric Key Exchange
QKD (optical short range only)
Quantum-safe Key Exchange Algorithm

Key Exchange Options

In-band
Out-of-band
Key exchange via DWDM (optical)
Key exchange via raw Ethernet
In-band key exchange via IP
- IPv4
- IPv6

Key System

Point-to-Point Key System

Supported key system
- Pairwise
- Group

Key assignment based on:
- MAC Address
- VLAN ID
- Port
- Group
- IP Address

Point-to-Multipoint Key System

Supported key systems:
- Pairwise
- Group

Key assignment based on:
- MAC Address
- VLAN ID
- Port
- Group
- IP Address

Multipoint Key System

Supported key systems:
- Pairwise
- Group
- Mixed (pairwise unicast, group multicast)

Key assignment based on:
- MAC address (pairwise and mixed)
- Multicast groups (mixed)
- VLAN ID (group)
- Port
- Group (group)
- IP Address
- IP Multicast Group

Individual key per multicast group

Individual key per broadcast group (VLAN ID)

Group Key System Specifics

Additional separate authentication per group

Group Membership Definition
- Multicast group membership
- Individual membership
- Network membership
- VLAN membership
- Trunked VLAN membership
- IP Address

Exclusion
- MAC address
- VLAN ID
- Frames with MPLS tag
- IP Address
- IP Muticast Group

Group Key Distribution
- Unicast (unique KEK per group member)
- Broadcast (same KEK for all group members)

Network Support

Bump in the Wire deployment

Jumbo Frame Support

Ethernet Flow Control via PAUSE

Tagging of untagged frames

Ethernet Fragmentation/Defragmentation
- Point-to-Point
- Point-to-Multipoint
- Multipoint

Dead Peer Detection

Optical Loss Pass-Through

Link Loss Carry Forward

System Configuration and Management Access

IPv4

IPv6

Out-of-band Management
- RS-232/V.24
- Separate Ethernet port

Smart Card (Secure Card) Support

USB Port

In-band Management
- SSH
- SNMP (read-only/read-write)
- TLS
- Proprietary

Remote Monitoring (SNMP)

Logs

Event Log (local)	
Audit Log (local)	
Syslog Support (Server)	

Unit

Height in 19" Rack	
Number of external encrypted Ethernet ports	
Physical Device Access	
Redundant Power Supply	
Redundant, hot-swappable power supply	
High Availability functionality (two-node cluster)	
MTBF	
Tamper Security	
Security Approvals	
Safety Approvals	
Boot Time	
Cold boot until operational (P2P)	
Warm boot until operational (P2P)	

Management Software

User Interface	Native PC application
	Embedded Webapp
	CLI
Initial Device Set-up	
	Local (out-of-band)
	Remote (out-of-band)
Device Configuration	
	Local (out-of-band)
	Remote (in-band)
	Remote (out-of-band)
Management Access	
	Role-based access
	Identity-based authentication of user
	Number of hierarchy levels
	Number of roles
	Strict internal separation of users
Device Management	
	Device Diagnostics
	Link Monitoring (SNMP)
	Connection Diagnostics
	In-band Network Diagnostics
	Remote Update/Upgrade
Certificate Authority & Management	
	Certificate Creation
	Certificate Management
Key Management	
	Group creation
	Group isolation
	Key assignment
	Fail-over configuration

Price

List Price Encryption Unit (in €)	
Per extermal Key Server (in €); optional, no requirement, starting price	
Required Management Software	
Optional SMC Sofware	1-4 encryptors
	5-10 encryptors
	11-20 encryptors
	unlimited
Warranty Period (months)	
Warranty Coverage	Parts & Work
	Basic Support (9 to 5, e-mail, phone)
	Software updates and upgrades
Warranty Extension (per year)	

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

Thales

	CV1000	CN4010	CN4020	CN6010	CN6100	CN6140	CN9120
Line Interface/Supported Line Rates							
10 Mbs							
100 Mps							
1 Gbps							
4x1 Gbps							
10 Gbps							
4x10 Gbps							
25Gps							
40 Gbps							
100 Gbps							
Virtual Appliance							
Supported Network Topologies							
Point-to-Point (P2P)							
Point-to-Multipoint (P2MP)							
Multipoint (MP)							
Supported Metro Ethernet Topologies							
Port-based							
Ethernet Private Line (EP-Line)							
Ethernet Private Tree (EP-Tree)							
Ethernet Private LAN (EP-LAN)							
VLAN-based							
Ethernet Virtual Private Line (EVP-Line)							
Ethernet Virtual Private Tree (EVP-Tree)							
Ethernet Virtual Private LAN (EVP-LAN)							
Supported Networks (Encryption)							
Ethernet							
MPLS (MPLSoE)							
MPLS (MPLSoIP)							
IPv4							
IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)							
MPLS (EoMPLS)							
IPv4 (including EoIP and MPLSoIP)							
TCP							
UDP							
IPv6 (including EoIP and MPLSoIP)							
TCP							
UDP							
Supported Usage Scenarios							
Single tenant							
Multi-tenant							
per-port							
per-VLAN							
Self-managed							
Managed encryption service							
Managed security service							

Platform

Platform used

- Mainboard/Firmware
- Key Management

Operating Modes

- P2P Mode
- Multipoint Mode

Data Plane Encryption Standard and Processing

Encryption Standard

- Block Cipher
- Preferred Mode of Operation
- Alternative Mode of Operation
- Key Length (in bit)

Processing Method

- cut-through
- store&forward

Encryption Hardware

- FPGA
- ASIC
- CPU

Latency

- Latency P2P Mode
  - cut-through
  - store & forward
- Latency MP Mode
  - cut-through
  - store & forward

Performance Documentation

- Ethernet Throughput & Latency Data available
- RFC 2544 Throughput & Latency Data available

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)

- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Counter length (in bytes)
- Registered Ethertype
- Frame overhead (unauthenticated encryption)
- Frame overhead (authenticated encryption)
- Ethernet multi-hop support

Transport (Payload only)

- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Definable encryption offset (fixed)
- Variable encryption offset
- Adaptive encryption offset based on frame content
- Registered EtherType
- Counter length (in bytes)
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Tunnel (Ethernet over Ethernet)

- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Registered Ethertype
- Counter length (in bytes)
- Frame overhead unauthenticated encryption
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)

- Supported transmission protocols (UDP/TCP)
- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Proprietary Ethertype
- Counter length (in bytes)
- Frame overhead unauthenticated encryption
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Native IP Encryption

Supported IP versions

- IPv4
- IPv6

Supported transmission protocols

- TCP
- UDP

Transport Mode

- Mximum number of peers
- Maximum number of IP addresses
- Maximum number of multicast groups
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - Additional Authenticated Data (header)
- Replay Protection
  - Variable replay window (size)
- Counter length (in bytes)
- Packet overhead authenticated encryption (AE)

Transport Tunnel Mode

- Maximum number of peers
- Maximum number of IP addresses
- Maximum number of multicast groups
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - Additional Authenticated Data (header)
- Replay Protection
  - Variable replay window (size)
- Counter length (in bytes)
- Packet overhead authenticated encryption (AE)

Selective Encryption

- Based on MAC Address
- Based on VLAN ID
- Based on Ethertype
- Based on Multicast Group
- Based on Presence of MPLS Tag
- Based on IP Address
- Combination of multiple selection criteria

Mixed Ethernet, MPLS, EoIP and IP Support

Based on VLAN ID

- MPLS
- EoIP
- IP

Based on presence of MPLS tag

- MPLS
- EoIP
- IP

Based on VLAN ID and presence of MPLS tag

- MPLS
- EoIP
- IP

Extended Security Features

Customizable AES S-Box

AES S-Box Customization

Traffic Masking

Traffic Flow Security

P2P
P2MP

Method

Configurable uniform frame size
Synthetic traffic injection

Control Plane

Control Plane Options

In-band
Out-of-band
Option to separate key exchange from control plane

Protection layer (in-band)

Ethernet (layer 2)
IP (layer 3)
Transport (layer 4)

Encryption Hardware (in-band)

FPGA
ASIC
CPU

Encryption (in-band)

Separate from data plane encryption
Same protection level as data plane encyption

DoS Resiliency (in-band)

line rate

Auto-discovery

Auto-discovery of network encryptors
Auto-discovery of key servers
Auto-discovery of VLANs
Disabling of auto-discovery

Key Server

Integrated Key Server
Support for external Key Server
External Key Server
Support for multiple distributed Key Servers
Support for fail-over to back-up Key Server

Autonomous operation

Key Management

Key Generation and Storage

Hardware Random Number Generation
Tamper Security Key Storage (tamper-evident or tamper-proof)

Asymmetric Key Algorithms (Public Key Cryptography)

RSA

Key length
Key strength (in bit)

Elliptic Curve Cryptography (ECC)

Key length
Key strength (in bit)

Supported Curves:

NIST
Brainpool
Custom Curves

Hash Algorithms

SHA-2
- Key length
- Key strenght (Image/Collision Resistance)

Device Authentication

Symmetric Signature: Pre-shared Key (PSK)
- Maximum number of PSKs per encryptor
- Key length
- Key strenght (in bit)

Asymmetric Signature: Certificate
- Maximum number of certificates per encryptor
- Key length
- Key strength (in bit)

Ad-hoc authentication of peers (manual)
Signature key protocol

Key Agreement and Key Exchange

Master Key (KEK) Agreement
Master Key (KEK) Exchange Protocol
Automatic Change of Master Key
Minimum suggested Time Interval for Master Key Change (min)
Separate Master Key (KEK) per site
Separate Master Key (KEK) per group

Session Key (DEK) Exchange Agreement
Session Key (DEK) Exchange Protocol
Automatic Change of Session Keys
Minimum Time Interval for Session Key Change (min)

Quantum-safe Key Exchange

Symmetric Encryption of Asymmetric Key Exchange
QKD (optical short range only)
Quantum-safe Key Exchange Algorithm

Key Exchange Options

In-band
Out-of-band
Key exchange via DWDM (optical)
Key exchange via raw Ethernet
In-band key exchange via IP
- IPv4
- IPv6

Key System

Point-to-Point Key System

Supported key system
- Pairwise
- Group

Key assignment based on:
- MAC Address
- VLAN ID
- Port
- Group
- IP Address

Point-to-Multipoint Key System

Supported key systems:
- Pairwise
- Group

Key assignment based on:
- MAC Address
- VLAN ID
- Port
- Group
- IP Address

Multipoint Key System

Supported key systems:
- Pairwise
- Group
- Mixed (pairwise unicast, group multicast)

Key assignment based on:
- MAC address (pairwise and mixed)
- Multicast groups (mixed)
- VLAN ID (group)
- Port
- Group (group)
- IP Address
- IP Multicast Group

Individual key per multicast group

Individual key per broadcast group (VLAN ID)

Group Key System Specifics

Additional separate authentication per group

Group Membership Definition
- Multicast group membership
- Individual membership
- Network membership
- VLAN membership
- Trunked VLAN membership
- IP Address

Exclusion
- MAC address
- VLAN ID
- Frames with MPLS tag
- IP Address
- IP Muticast Group

Group Key Distribution
- Unicast (unique KEK per group member)
- Broadcast (same KEK for all group members)

Network Support

Bump in the Wire deployment

Jumbo Frame Support

Ethernet Flow Control via PAUSE

Tagging of untagged frames

Ethernet Fragmentation/Defragmentation
- Point-to-Point
- Point-to-Multipoint
- Multipoint

Dead Peer Detection

Optical Loss Pass-Through

Link Loss Carry Forward

System Configuration and Management Access

IPv4

IPv6

Out-of-band Management
- RS-232/V.24
- Separate Ethernet port

Smart Card (Secure Card) Support

USB Port

In-band Management
- SSH
- SNMP (read-only/read-write)
- TLS
- Proprietary

Remote Monitoring (SNMP)

Logs

Event Log (local)	
Audit Log (local)	
Syslog Support (Server)	

Unit

Height in 19" Rack	
Number of external encrypted Ethernet ports	
Physical Device Access	
Redundant Power Supply	
Redundant, hot-swappable power supply	
High Availability functionality (two-node cluster)	
MTBF	
Tamper Security	
Security Approvals	
Safety Approvals	
Boot Time	
Cold boot until operational (P2P)	
Warm boot until operational (P2P)	

Management Software

User Interface	Native PC application
	Embedded Webapp
	CLI
Initial Device Set-up	
	Local (out-of-band)
	Remote (out-of-band)
Device Configuration	
	Local (out-of-band)
	Remote (in-band)
	Remote (out-of-band)
Management Access	
	Role-based access
	Identity-based authentication of user
	Number of hierarchy levels
	Number of roles
	Strict internal separation of users
Device Management	
	Device Diagnostics
	Link Monitoring (SNMP)
	Connection Diagnostics
	In-band Network Diagnostics
	Remote Update/Upgrade
Certificate Authority & Management	
	Certificate Creation
	Certificate Management
Key Management	
	Group creation
	Group isolation
	Key assignment
	Fail-over configuration

Price

List Price Encryption Unit (in €)	
Per extermal Key Server (in €); optional, no requirement, starting price	
Required Management Software	
Optional SMC Sofware	1-4 encryptors
	5-10 encryptors
	11-20 encryptors
	unlimited
Warranty Period (months)	
Warranty Coverage	Parts & Work
	Basic Support (9 to 5, e-mail, phone)
	Software updates and upgrades
Warranty Extension (per year)	

2022 Market Overview Layer 2 Encryption: For Carrier Ethernet, MPLS and IP

MACSec EDE

	Virtual Appliance	Appliance
Line Interface/Supported Line Rates		
10 Mbs		
100 Mps		
1 Gbps		
10 Gbps		
25Gps		
40 Gbps		
100 Gbps		
Virtual Appliance	✓	
Supported Network Topologies		
Point-to-Point (P2P)	✓	✓
Point-to-Multipoint (P2MP)	✓	✓
Multipoint-to-Multipoint/Mesh (MP)		
Supported Metro Ethernet Topologies		
Port-based		
Ethernet Private Line (EP-Line)	✓	✓
Ethernet Private Tree (EP-Tree)	✓	✓
Ethernet Private LAN (EP-LAN)	✓	✓
VLAN-based		
Ethernet Virtual Private Line (EVP-Line)	✓	✓
Ethernet Virtual Private Tree (EVP-Tree)	✓	✓
Ethernet Virtual Private LAN (EVP-LAN)	✓	✓
Supported Networks (Encryption)		
Ethernet	✓	✓
MPLS (MPLSoE)	✓	✓
MPLS (MPLSoIP)		
IPv4		
IPv6		
Supported Networks (Transport of Encrypted Frame)		
Ethernet (native)	✓	✓
MPLS (EoMPLS)	✓	✓
IPv4 (including EoIP and MPLSoIP)		
TCP		
UDP		
IPv6 (including EoIP and MPLSoIP)		
TCP		
UDP		
Supported Usage Scenarios		
Single tenant	✓	✓
Multi-tenant		
per port		
per VLAN-ID		
Self-managed	✓	✓
Managed encryption service		
Managed security service		

Platform

Platform used			
	Mainboard/Firmware		
	Key Management	MKA/EAPOL-TLS	MKA/EAPOL-TLS
Operating Modes			
	P2P Mode	✓	✓
	Multipoint Mode	✓	✓

Data Plane Encryption Standard and Processing

Encryption Standard			
	Block Cipher	AES	AES
	Preferred Mode of Operation	GCM	GCM
	Alternative Mode of Operation		
	Key Length (in bit)	256	256
Processing Method			
	cut-through		
	store&forward	✓	✓
Encryption Hardware			
	FPGA		
	ASIC		
	CPU	✓	
Latency			
Latency P2P Mode	cut-through		
	store & forward		
Latency MP Mode	cut-through		
	store & forward		
Performance Documentation			
Ethernet Throughput & Latency Data available			
RFC 2544 Throughput & Latency Data available			

Encryption Modes

Native Ethernet Encryption

Frame Encryption (Bulk - P2P only)			
	Integrity protection (algorithm)		
	Authentication length (bytes)		
	AAD (additional authenticated data)		
	Replay protection		
	Variable replay window (size)		
	Counter length (in bytes)		
	Registered Ethertype		
	Frame overhead (authenticated encryption)		
Transport (Payload only)		✓	✓
	Max. number of peers	32 - Expandable to 256	32 - Expandable to 256
	Max. number of MAC Addresses	unlimited	unlimited
	Max. number of VLAN IDs	unlimited	unlimited
	Integrity protection (algorithm)	GCM	GCM
	Authentication length (bytes)	16	16
	AAD (additional authenticated data)	✓	✓
	Replay protection	✓	✓
	Variable replay window (size)	≤ 2^31-1 frames/time	≤ 2^31-1 frames/time
	Definable encryption offset (fixed)	✓	✓
	Variable encryption offset	✓	✓
	Adaptive encryption offset based on frame content		
	Registered EtherType	MACSec Ethertype	MACSec Ethertype
	Counter length (in bytes)	8	8
	Frame overhead authenticated encryption (AEAD)	32	32
	Ethernet multi-hop support	✓ (dependent on type of hop)	✓ (dependent on type of hop)
Tunnel (Ethernet over Ethernet)		✓ (next version)	✓ (next version)
	Max. number of peers		
	Max. number of MAC Addresses		
	Max. number of VLAN IDs		
	Integrity protection (algorithm)		
	Authentication length (bytes)		
	AAD (additional authenticated data)		
	Replay protection		
	Variable replay window (size)		
	Registered Ethertype		
	Counter length (in bytes)		
	Frame overhead authenticated encryption (AEAD)		
	Ethernet multi-hop support		

Ethernet over IP (EoIP)

Tunnel (Ethernet over IP)

- Supported transmission protocols (UDP/TCP)
- Max. number of peers
- Max. number of MAC Addresses
- Max. number of VLAN IDs
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - AAD (additional authenticated data)
- Replay protection
  - Variable replay window (size)
- Proprietary Ethertype
- Counter length (in bytes)
- Frame overhead authenticated encryption (AE)
- Ethernet multi-hop support

Native IP Encryption

Supported IP versions

- IPv4
- IPv6

Supported transmission protocols

- TCP
- UDP

Transport Mode

- Maximum number of peers
- Maximum number of IP addresses
- Maximum number of multicast groups
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - Additional Authenticated Data (header)
- Replay Protection
  - Variable replay window (size)
- Counter length (in bytes)
- Packet overhead authenticated encryption (AE)

Transport Tunnel Mode

- Maximum number of peers
- Maximum number of IP addresses
- Maximum number of multicast groups
- Integrity protection (algorithm)
  - Authentication length (bytes)
  - Additional Authenticated Data (header)
- Replay Protection
  - Variable replay window (size)
- Counter length (in bytes)
- Packet overhead authenticated encryption (AE)

Selective Encryption

- Based on MAC Address
- Based on VLAN ID
- Based on Ethertype
- Based on Multicast Group
- Based on Presence of MPLS Tag
- Based on IP Address
- Combination of multiple selection criteria

Mixed Ethernet, MPLS, EoIP and IP Support

Based on VLAN ID			
	MPLS	✓	✓
	EoIP		
	IP		
Based on presence of MPLS tag			
	MPLS	✓	✓
	EoIP		
	IP		
Based on VLAN ID and presence of MPLS tag			
	MPLS	✓	✓
	EoIP		
	IP		

Extended Security Features			
AES S-box customization			
Customizable AES S-box			
Traffic Masking			
Traffic Flow Security			
	P2P		
	P2MP		
Method			
	Uniform frame size	✓ (next version)	✓ (next version)
	Synthetic traffic injection		
Control Plane			
Control Plane Options			
	In-band	Key Exchange Status and Management	Key Exchange Status and Management
	Out-of-band		
	Option to separate key exchange from control plane		
Protection layer (in-band)			
	Ethernet (layer 2)		
	IP (layer 3)		
	Transport (layer 4)	✓	✓
Encryption Hardware (in-band)			
	FPGA		✓
	ASIC		
	CPU	✓	
Encryption (in-band)			
	Separate from data plane encryption	✓	✓
	Same protection level as data plane encyption		
DoS Resiliency (in-band)			
	line rate		
Auto-discovery			
Auto-discovery of network encryptors		✓	✓
Auto-discovery of key servers		✓	✓
Auto-discovery of VLANs			
Disabling of auto-discovery		✓	✓
Key Server			
Integrated Key Server		✓	✓
Support for external Key Server			
External Key Server			
Support for multiple distributed Key Servers		✓	✓
Support for fail-over to back-up Key Server		✓	✓
Autonomous operation		✓	✓
Key Management			
Key Generation and Storage			
Hardware Random Number Generation			✓
Tamper Security Key Storage (tamper-evident or tamper-proof)			TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)			
Elliptic Curve Cryptography (ECC)			
	Key length	384	384
	Key strength (in bit)	192	192
Supported Curves:			
	NIST	✓	✓
	Brainpool		
	Custom Curves		
Hash Algorithms			
SHA-2	Key length	512	512
	Key strength (Image/Collision Resistance)	512/256	512/256

Device Authentication			
Symmetric Signature: Pre-shared Key (PSK)		✓	✓
	Maximum number of PSKs per encryptor		
	Key length	256	256
	Key strenght (in bit)		
Asymmetric Signature: Certificate		x.509	x.509
	Maximum number of certificates per encryptor	1	1
	Key lenght	384	384
	Key strenght (in bit)	192	192
Ad-hoc authentication of peers (manual)			
Signature key protocol		ECDSA	ECDSA
Key Agreement and Key Exchange			
Master Key (KEK) Agreement		TLS 1.2/TLS 1.3	TLS 1.2/TLS 1.3
Master Key (KEK) Exchange Protocol		EAP	EAP
Automatic Change of Master Key		✓	✓
Minimum suggested Time Interval for Master Key Change (min)		60	60
Separate Master Key (KEK) per site		✓	✓
Separate Master Key (KEK) per group			
Session Key (DEK) Exchange Agreement		MKA	MKA
Session Key (DEK) Exchange Protocol		EAP	EAP
Automatic Change of Session Keys		✓	✓
Minimum Time Interval for Session Key Change (min)			
Key Exchange Options			
In-band		✓	✓
Out-of-band			
Key exchange via DWDM (optical)			
Key exchange via raw Ethernet		✓	✓
In-band key exchange via IP	IPv4		
	IPv6		
Key System			
Point-to-Point Key System			
Supported key system			
	Pairwise	✓	✓
	Group		
Key assignment based on:			
	MAC Address	✓	✓
	VLAN ID	✓	✓
	Port		✓
	Group	✓	✓
	IP Address		
Point-to-Multipoint Key System			
Supported key systems:			
	Pairwise	✓	✓
	Group	unidirectional group	unidirectional group
Key assignment based on:			
	MAC Address	✓	✓
	VLAN ID	✓	✓
	Port	✓	✓
	Group	✓	✓
	IP Address		

Multipoint Key System			
Supported key systems:			
	Pairwise	✓	✓
	Group	unidirectional group	unidirectional group
	Mixed (pairwise unicast, group multicast)		
Key assignment based on:			
	MAC address (pairwise and mixed)		
	Multicast groups (mixed)		
	VLAN ID (group)		
	Port		
	Group (group)		
	IP Address		
	IP Multicast Group		
Individual key per multicast group			
Individual key per broadcast group (VLAN ID)			
Group Key System Specifics			
Additional separate authentication per group			
Group Membership Definition			
	Multicast group membership		
	Individual membership	✓	✓
	Network membership		
	VLAN membership		
	Trunked VLAN membership		
	IP Address		
Exclusion			
	MAC address		
	VLAN ID		
	Frames with MPLS tag		
	IP Address		
	IP Muticast Group		
Group Key Distribution			
	Unicast (unique KEK per group member)		
	Broadcast (same KEK for all group members)		
Network Support			
Bump in the Wire deployment		✓	✓
Jumbo Frame Support		✓	✓
Ethernet Flow Control via PAUSE			
Tagging of untagged frames			
Ethernet Fragmentation/Defragmentation			
	Point-to-Point		
	Point-to-Multipoint		
	Multipoint		
Dead Peer Detection		✓	✓
Optical Loss Pass-Through			
Link Loss Carry Forward			
System Configuration and Management Access			
IPv4		✓	✓
IPv6			
Out-of-band Management		✓	✓
	RS-232/V.24		
	Separate Ethernet port	✓	✓
Smart Card (Secure Card) Support			
USB Port			
In-band Management			
	SSH	✓	✓
	SNMP (read-only/read-write)		✓
	TLS		
	Proprietary		
Remote Monitoring (SNMP)		v3	v3
Logs			
Event Log (local)		✓	✓
Audit Log (local)		✓	✓
Syslog Support (Server)		✓	✓

Unit

Height in 19" Rack			1
Number of external encrypted Ethernet ports			
Physical Device Access			
Redundant Power Supply			
Redundant, hot-swappable power supply			
High Availability functionality (two-node cluster)			
MTBF			
Tamper Security		N/A	TE/TP
Security Approvals			FIPS-140-2 Level 3, NIAP/CC EAL-4+, NSA Type 1
Safety Approvals			(can be achieved)
Boot Time			
	Cold boot until operational (P2P)		
	Warm boot until operational (P2P)		

Management Software

User Interface	Native PC application		
	Embedded Webapp		
	CLI		
Initial Device Set-up			
	Local (out-of-band)		
	Remote (out-of-band)		
Device Configuration			
	Local (out-of-band)		
	Remote (in-band)		
	Remote (out-of-band)		
Management Access			
	Role-based access	✓	✓
	Identity-based authentication of user	✓	✓
	Number of hierarchy levels	3	3
	Number of roles	2	2
	Strict internal separation of users		
Device Management			
	Device Diagnostics	✓	✓
	Link Monitoring (SNMP)	✓	✓
	Connection Diagnostics	✓	✓
	In-band Network Diagnostics	✓	✓
	Remote Update/Upgrade	✓	✓
Certificate Authority & Management			
	Certificate Creation		
	Certificate Management		
Key Management			
	Group creation		
	Group isolation		
	Key assignment		
	Fail-over configuration		

Price

List Price Encryption Unit (in €)			
Per external Key Server (in €)			
Required Management Software			
	2-10 encryptors		
	11-25 encryptors		
	26-50 encryptors		
	51+ encryptors		
Warranty Period (months)			
Warranty Coverage	Parts & Work		
	Basic Support (9 to 5, e-mail, phone)		
	Software updates and upgrades		
Warranty Extension (per year)			

MACsec comes in different variants. There are many proprietary implementations of the standard. Interoperability between those implementations is not a given.
There is only a cPP for point-to-point, but none for point-to-multipoint and none for multipoint (mesh)
The scope of the cPP does not cover the security of the AAA server