inside-it.ch

PRESENTS:

LAYER 2-ENCRYPTORS FOR METRO AND CARRIER ETHERNET WANS AND MANS

MARKET OVERVIEW ETHERNET ENCRYPTORS FOR CARRIER ETHERNET, MPLS AND IP NETWORKS

(SHORT VERSION)

Version 6.1, June 7, 2017

www.uebermeister.com
cjaggi@uebermeister.com

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.

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 substantial increase in demand for layer 2 encryptors has a simple reason: Efficiency paired with cost savings. Over 99.9 percent of all network attacks target layer 3 to 7. Encrypting connections between sites at layer 2 prevents successful attacks, if the encryption is properly implemented. If authenticated encryption is used, then the benefits of encryption are not limited to data confidentiality, as the mechanism also provides intrusion detection, intrusion prevention, and firewalling at layer 2. The combination of security and efficiency is the reason for the rapidly increasing adoption of dedicated layer 2 encryption appliances. Some customers of such solutions are already operating up to 500 devices 24/7/365.

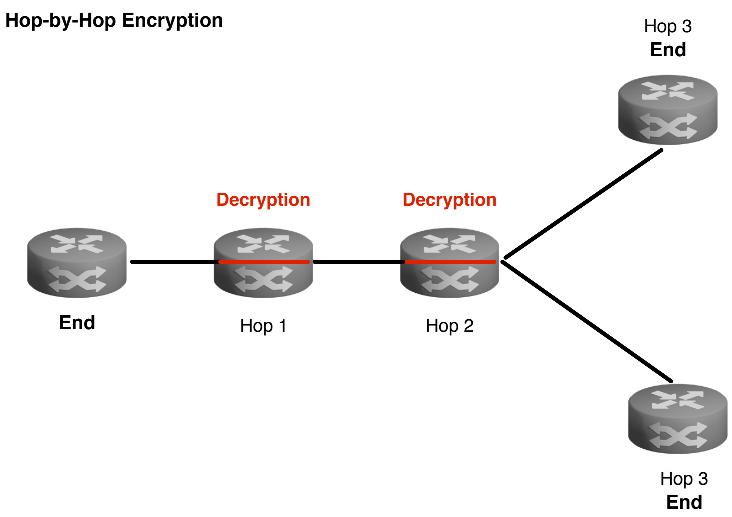
2. Different approaches

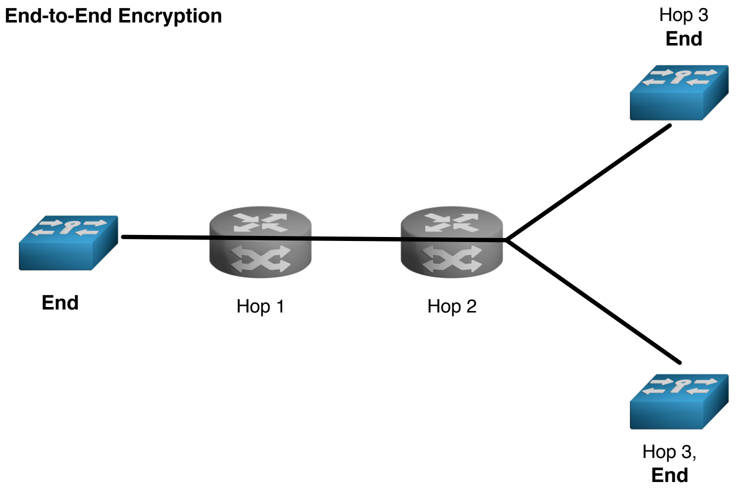
For network encryption there are different approaches and practices. They have a direct impact on the application scenarios supported and the security level provided by a solution.
There are different possibilities to encrypt Ethernet networks. It can be done at layer 1, layer 2 and layer 3. It is most 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 endpoint 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. While the first MACSec-based dedicated appliances based on the NSA Ethernet Security Specifications (ESS) and IEEE 802.1AEcg specifications are becoming available on the market, they deviate from the IEEE 802.1AE standard in order to support more Carrier Ethernet environments. These devices use FPGAs instead of ASICs, but inherit most of the shortcomings of MACSec, including the key management. In terms of network support, security and scalability they are still way behind most dedicated devices that have been developed specifically for the protection of Carrier Ethernet networks. ESS is work in progress and IEEE 802.1AEcg is still not finalized despite being years in the making. The standards for Carrier Ethernet security are set by the dedicated encryption appliances that have been available for over a decade. The devices that profited from ongoing development efforts have reached a high level of maturity and are widely deployed, setting the de-facto standards.

There is no standard for the end-to-end encryption for Metro and Carrier Ethernet and MPLS networks, but there are well-established and proven methods for the encryption of data networks that can be applied to Metro and Carrier Ethernet and MPLS networks while taking into account the specific requirements for the respective network type. The different vendors are using different approaches, both on the control and the data plane. The different market offers thus create a confusing and unclear situation. This market overview tries to make the different approaches comparable. It can however not make the quality of the implementation of the different offers comparable or assessable.

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, 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 and 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 securing Carrier-Ethernet networks end-to-end. The different vendors use different approaches for securing the data and the control plane, making it hard to get a clear understanding of what is available on the market. This market overview tries to make the different offers comparable. Integrated solutions based on MACSec are not part of this market overview as MACSec is not an end-to-end but a hop-by-hop encryption. The vast majority of MACSec-based solutions is integrated into switches and routers and is using proprietary modifications to overcome at least some of the limitations of the IEEE standard for LANs. These modifications make the different MACSec implementations non-interoperable.

This market overview shows different approaches to securing Metro and Carrier Ethernet MANs and WANs. 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 cost. The product selection has an impact on security, compatibility, efficiency, flexibility and ongoing cost.

The objective is to show the current and planned market offer in terms of functionality from a vendor point of view. Products and approaches are not rated.

3.2. Coverage

For this market overview, all of the important and relevant vendors have provided detailed information. Five factors define the market relevance: The market acceptance, the installed base, the current sales volume, the state of the security and network support and the breadth of the offer. Not included are therefore vendors whose products miss essential security functions such as authenticated encryption, don't provide native Ethernet encryption, offer limited Carrier Ethernet support or don't have the product breadth to cover the relevant bandwidth scenarios from 100Mb to 10Gb. Also not included are Carrier devices, such as Ethernet Access Devices, that can only encrypt the network data once the unencrypted network data has been handed over to the Carrier. For trustworthy network security encryption must take place before the network data is handed over to the Carrier.

In terms of MACSec, the coverage is limited to devices following the IEEE 802.1AEcg draft as this draft is for client-side appliances. IEEE 802.1AEcg deviates from IEEE 802.1AE in many areas, defines five device categories, and remains stuck with MKA (MACSec Key Agreement). From an engineering and product point of view it would have probably been a better decision to define a new standard for Carrier Ethernet encryption including a well-suited key management than to try to make a LAN-standard work with the completely different requirements of securing Carrier Ethernet networks. 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.

3. Objective

The objective of this market overview is to show the current and the planned products of the different vendors in a structured and detailed way. It shows the different approaches and possibilities to secure Carrier Ethernet MANs and WANs. The security and functionality requirements are determined by the usage scenario. Product functionality and the overall security provided are the most important evaluation criteria, followed by the acquisition and operating cost. The product selection has an impact on security, compatibility, efficiency, flexibility and consequential costs.

This market overview makes no recommendations in terms of vendor and platform. It provides however all information necessary to create a shortlist for an RFI or an RFP.

This market overview is one documents out of a series of three, which also includes an introduction into the encryption for Metro and Carrier Ethernet networks and an evaluation guide. Each document has a different focus and different content. Together, these three documents provide essential information and help for evaluating different solutions. The download is free and no registration is required.

http://www.uebermeister.com/files/inside-it/2016_Introduction_Encryption_Metro_and_Carrier_Ethernet.pdf

http://www.uebermeister.com/files/inside-it/2014_Evaluation_Guide_Encryptors_Carrier_and_Metro_Ethernet.pdf

The MANs and WANs used can differ as substantially as the security requirements. There are different approaches to serve the different needs and demands.

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 vendors covered:

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

Gemalto
(https://safenet.gemalto.com/data-encryption/network-encryption)

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

Rohde & Schwarz Cybersecurity
(https://cybersecurity.rohde-schwarz.com/en/products/secure-networks/ethernet-encryption-rsr-sitline-eth)

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

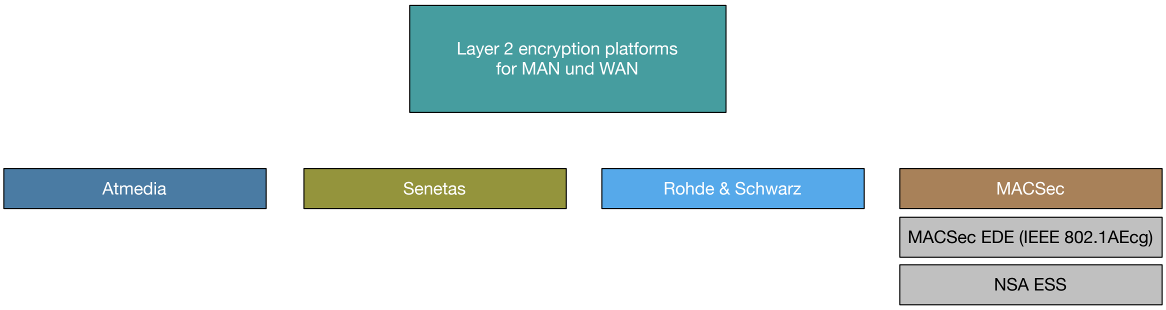
Securosys
(https://www.securosys.ch/layer-2-encryptor-centurion)

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

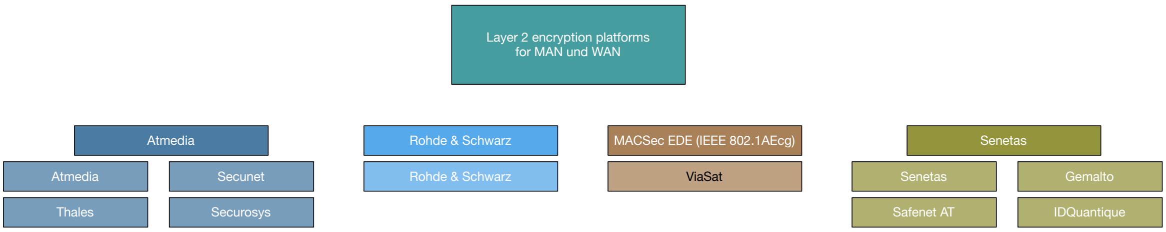
Thales
(https://www.thales-esecurity.com/products-and-services/products-and-services/network-encryption-appliances/datacryptor-5000-series)

ViaSat
(https://www.viasat.com/products/data-in-transit-encryption-for-enterprises)

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



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



The common denominator of the products is limited to the fact that they can encrypt Carrier Ethernet natively and authenticated. Except for the use of AES-GCM each platform does it differently and with different levels of network support. As the devices are network encryptors, the network support is as important as the encryption itself. On top, security technology and networks are subject to changing requirements and new carrier offers. Encryptors must be able to adapt to this evolution. Not all of them can. A limited flexibility of the encryptor normally leads to higher cost. Appliances based on FPGAs or CPUs can be undated and upgraded to adapt to new security and network requirements. The higher the flexibility of an encryption appliance, the higher the number of supported usage scenarios.

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 – mostly 40Gb/s and 100Gb/s devices – have multiple ports that – depending on vendor implementation – can be encrypted individually or combined.

The effective data throughput is not only determined by the network interface and the supported bandwidth, but also the frame overhead, the frame forwarding efficiency, and the processing power of the encryptor. Parameters such as encryption standard, encryption hardware, encryption mode and operating mode can have a noticeable impact on the actual throughput.

A limited number of vendors also offer their layer 2 encryptors as virtual appliances. Their security and performance depends 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 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. 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

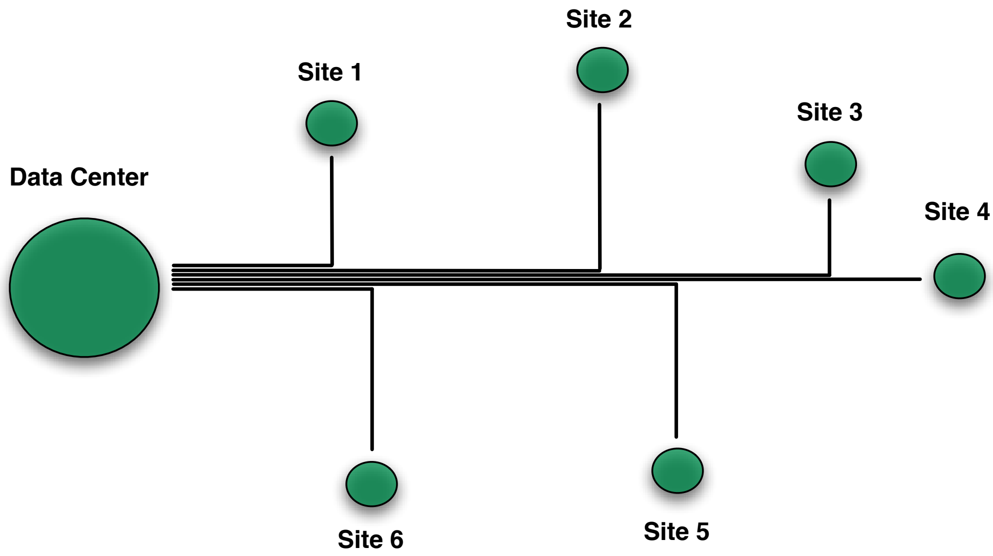
Key system and available encryption modes are defining factors for the support of different network topologies and Metro and Carrier Ethernet standards.

2.2.1. Point-to-Point

A point-to-point connection connects two sites.

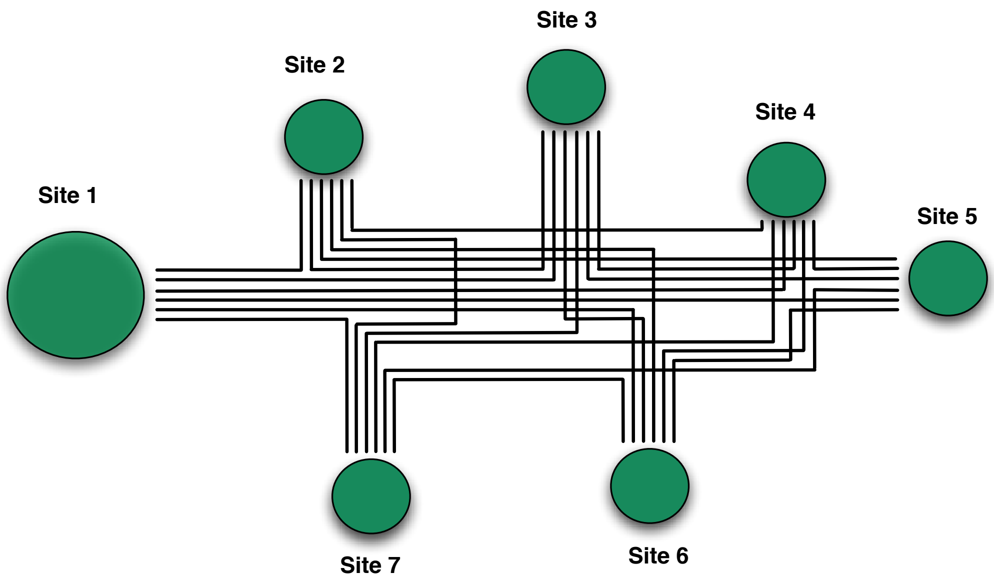
2.2.2. Point-to-Multipoint

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



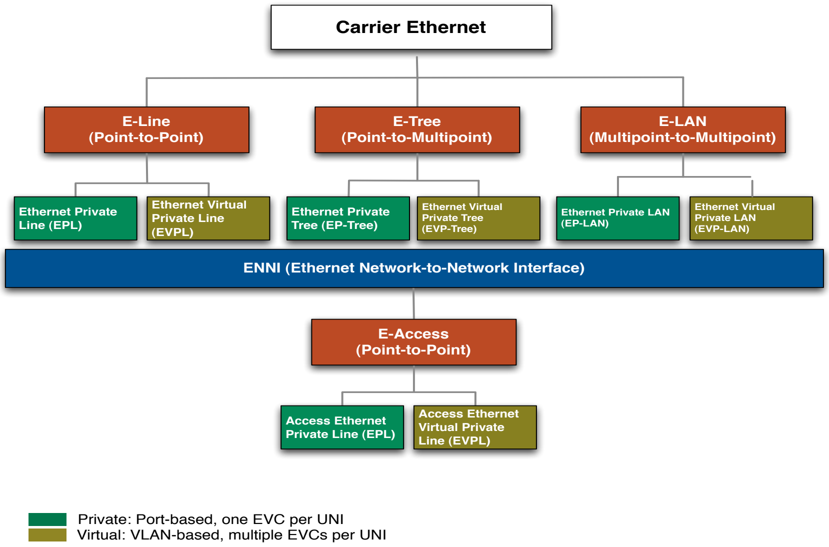
2.2.3. Multipoint-to-Multipoint

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

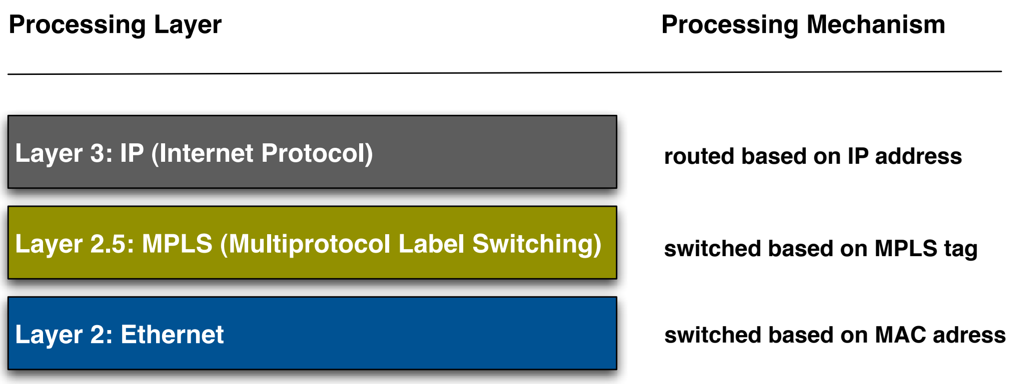
Encryption mode and key management are decisive factors for the proper support of the different MEF topologies.



2.4. Networks Supported for Encryption

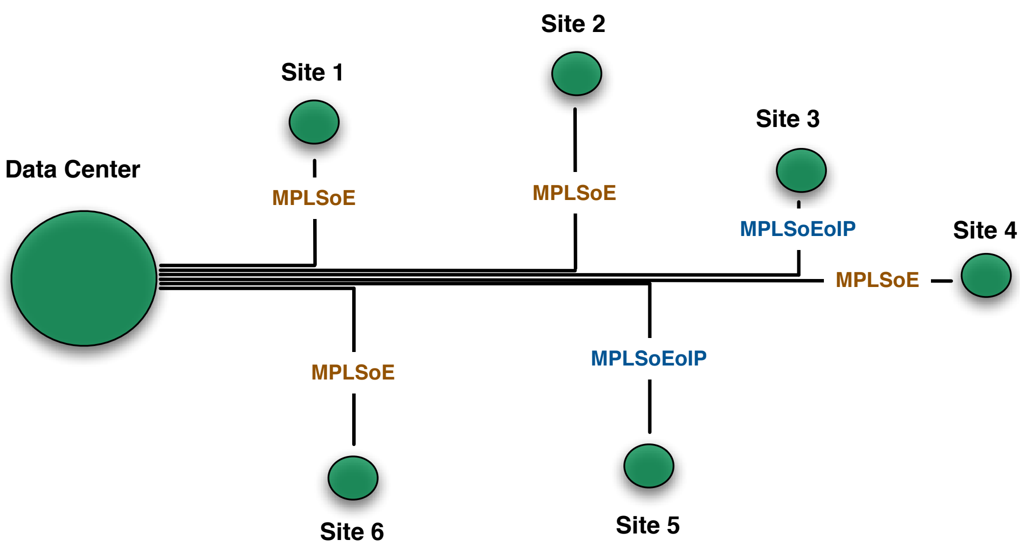
Carrier Ethernet can be viewed as layer 2 VPN, as network service for MPLS and IP networks and as access ramp to the public internet. Even as the combination of all of them. Most of the products focus on Ethernet and layer 2 VPNs as each of the networks used for multi-site connectivity - Ethernet, MPLS 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 only few offers on the market that support and protect all networks natively 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. Many 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.

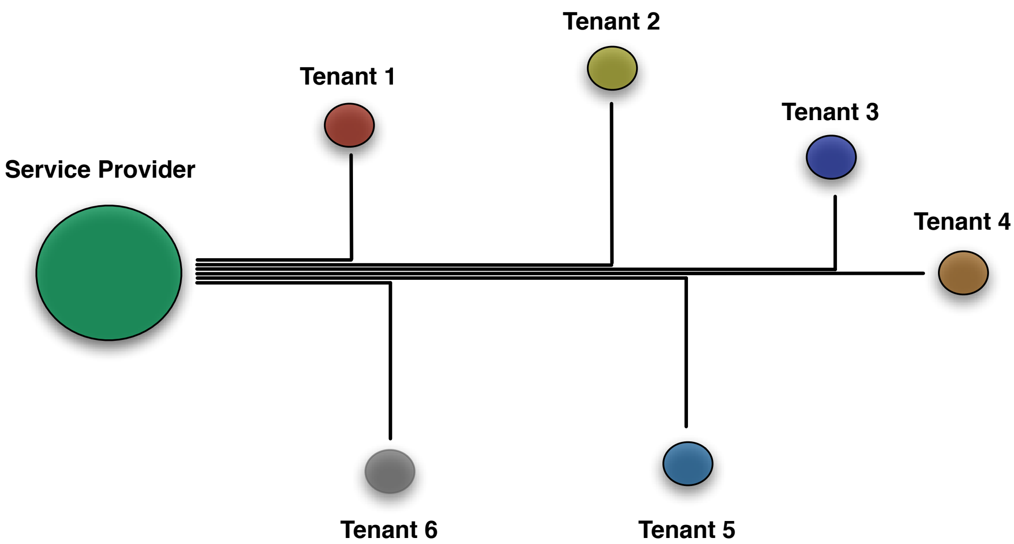


The demands in terms of encryptor functionality are substantially increased, as next to the frame transport over IP also key exchange over IP has to be supported.

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 connection of multiple different customers. This requires multi-tenancy support by the management software and the key system.



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.
Using pre-shared secrets is much simpler and efficient in such an environment.

2.7. Platform Used

The number of vendors surpasses the number of 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 the IEEE 801.2AEcg draft.
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. 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 vast majority of dedicated layer 2 encryption appliances sold and deployed worldwide with a market penetration of more than 90%. 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 seven years ago the most widely used block modes were Cipher-Block-Chaining (CBC) and the closely related Cipher-Feedback (CFB). In the meantime, the industry has moved to authenticated encryption and 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 intrusion detection, intrusion prevention and 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, which is also what MACSec, the IEEE standard for hop-by-hop encryption for campus-internal Ethernet networks uses. AES-GCM adds a frame overhead of 24-32 bytes, which is low compared to encryption at layer 3 (IPSec) and in relation to the added security.
Authentication, and replay and integrity protection play an increasingly important role in hop-by-hop and multi-hop networks, leading to a fast adoption of standards such as Galois Counter Mode (GCM). Today, enterprise-grade, government-grade and defense-grade encryption should use authenticated encryption with integrity and replay protection such as AES-GCM.

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.

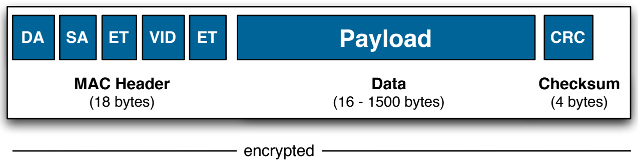
The encryption mode often has an impact on the scalability. A multipoint WAN can theoretically consist of thousands of sites, with the traffic between the sites handled by an encryptor at every site. In reality such large networks will be impossible to find, as a reasonable segmentation is the foundation 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.

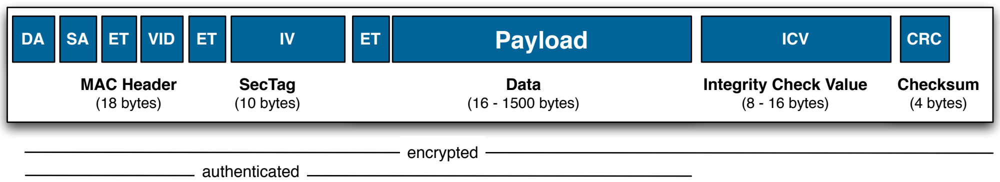
The frame diagrams below distort the ratio between header/CRC and payload heavily to the disadvantage of the header and checksum.

3.6.1. Frame Mode

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



Frame mode without authenticated encryption



Frame mode with authenticated encryption

Advantages:

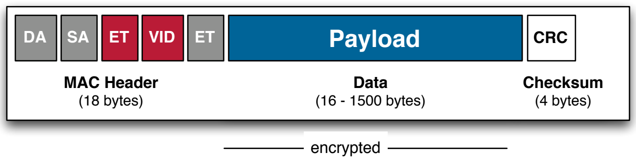
- All frames are completely encrypted
- Tapping the line will reveal nothing concerning network and data
- Authenticated encryption generates little overhead (24-32 bytes) compared to the security gained
- If unauthenticated, there is no encryption overhead on frame level

Disadvantages:

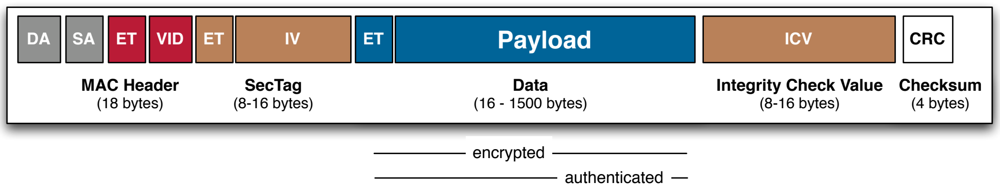
- Needs dedicated line
- Cannot be switched
- Has higher operating cost
- Incompatible with Managed Ethernet Services

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 unauthenticated encryption



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

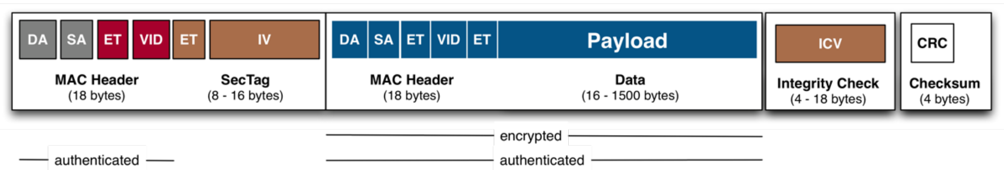
Disadvantages:

- 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.

Frame without frame-based explicit replay- and integrity protection



Frame with frame-based explicit replay- and integrity protection

Advantages:

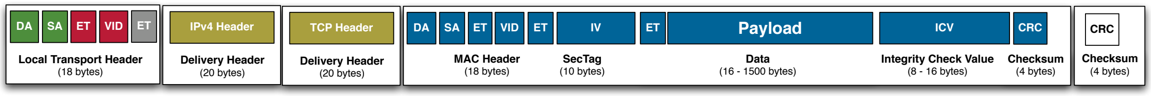
- Original frame is completely encrypted
- Can be switched
- Transparent to VLAN and MPLS
- Does not require dedicated line
- Compatible with Managed Ethernet Services

Disadvantages:

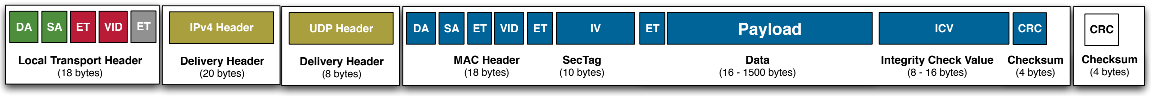
- Encryption overhead of up to 70% on frame level (with 64 byte frames), but averaging less than 10% in typical IMIX)
- Increases processing requirements
- Primarily optimized for point-to-point and point-to-multipoint
- Reduced scalability

3.6.4. 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

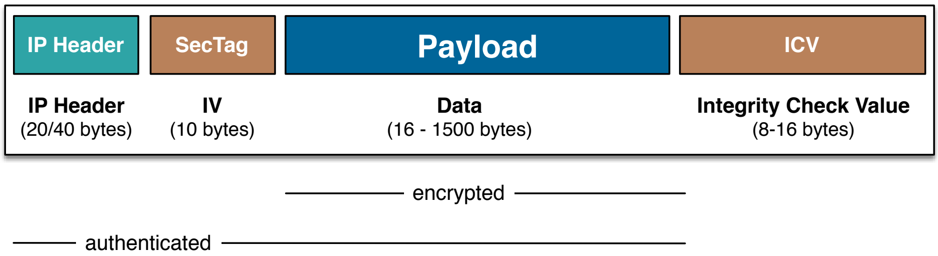


Ethernet over IP (EoIP) over UDP with authenticated encryption

If within the IP tunneling the entire original Ethernet frame, then the protection of the payload is similar to that of a bulk encryption. It is also 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.

3.6.5. Native IP Encryption

It is also possible to encrypt pure IP-networks from layer 2. It is however mandatory to factor in the characteristics and requirements of layer 3 networks.



Compared with IPSec-based solutions the encryption overhead is substantially lower and group key systems are available from the outset. Encryptors with native IP support are often used when a more secure and more performant alternative to GET VPN is needed.

3.7. Size of the Replay Window

Authenticated encryption 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.

3.8. 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, CoS, MPLS tag, Ethertype and MAC address. It is also possible to use factors such as 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. Further criteria that would be imaginable are e.g. Ethertype and CoS. Many Metro 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.

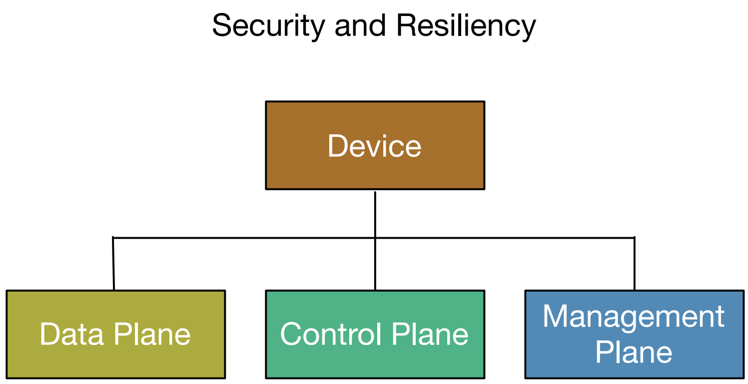
3.9. Traffic Flow Security

Traffic flow security obfuscates the actual data traffic by changing frame sizes and frame sequences during transport. Traditional methods were limited to using uniform frame sizes and to dedicated point-to-point scenarios. Newer methods work with variable frame sizes and support all usage scenarios. Some of them additionally use traffic flow optimization to offset the overhead penalty and manage to maintain the same IMIX throughput in tunnel mode (Ethernet tunnel or IP tunnel) as normally only attained in authenticated transport mode.

At this time, only two platforms offer traffic flow security, with one of the implementations using the traditional method. By allowing the definition and use of an 80 bytes transport header, this implementation works over different transport networks, including IP. The other implementation uses a newer method that supports all usage scenarios (point-to-point, point-to-multipoint and multipoint-to-multipoint), works over different transport networks and includes traffic flow optimization, providing full IMIX throughput in tunnel mode.

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 level of security and resilience required.

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 wants 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 Equipment

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

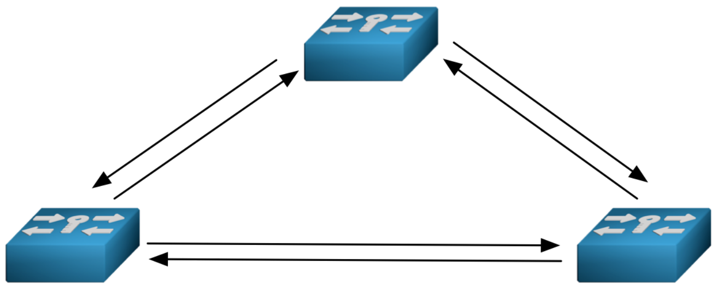
6.1.3. Autonomous Operation

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.

Connectivity Association

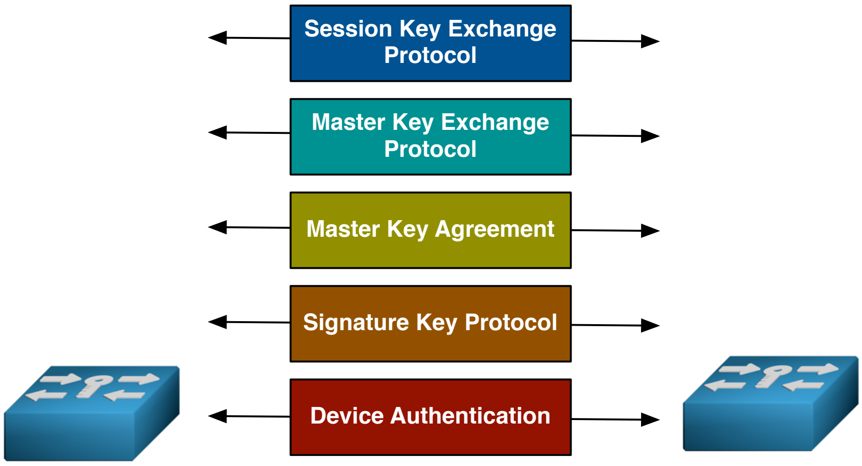


Establishment of permitted device connectivity

Authentication through certtificate or pre-shared key/pre-shared secret

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 dependant on the curves used. Among experts the security of the NIST curves is severely in doubt. 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 highly complex and also the proper implementation of elliptic curve cryptography is non-trivial. There are also speed differences between the different elliptic curves, but for multisite networks they do not 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. 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.

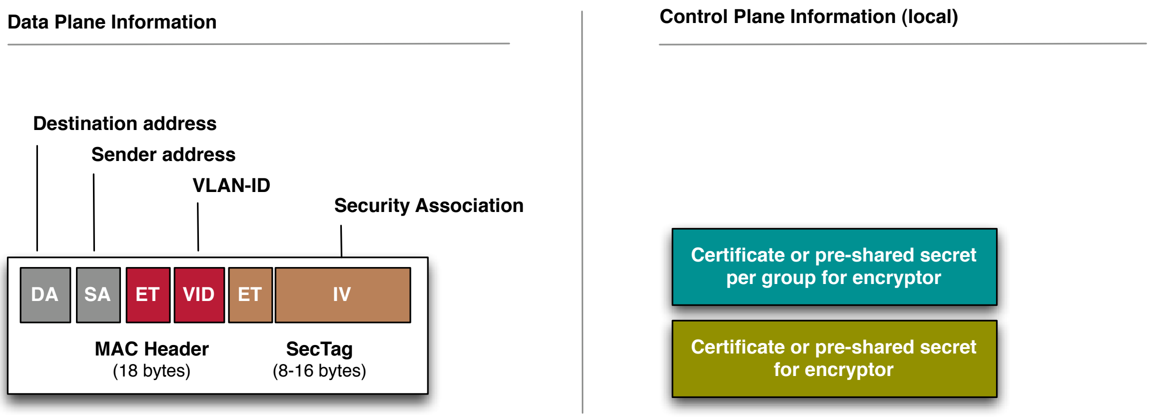
Key Type	Change Frequency
Session Key (Data Encryption Key)	every 1 - 60 minutes
Master Key (Key Encryption Key)	every 1 -24 hours
Initial Secret	every 12 - 24 months

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.

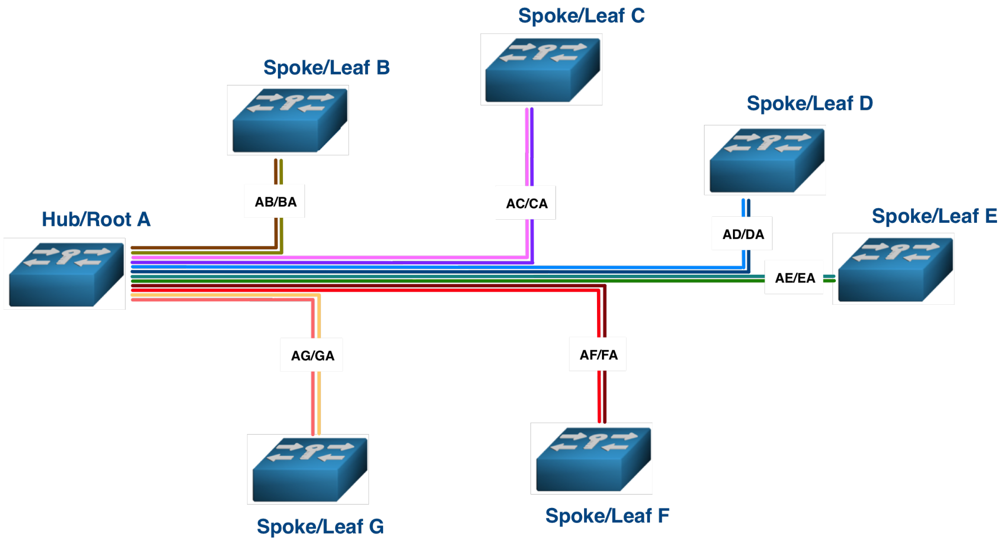
For pairwise key system a network consists of a multitude of point-to-point connections. Each encryptor is connected with each other encryptor by a point-to-point connection. Traditional pairwise key systems use unidirectional keys for the connection between a pair of encryptors.
Group key systems are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

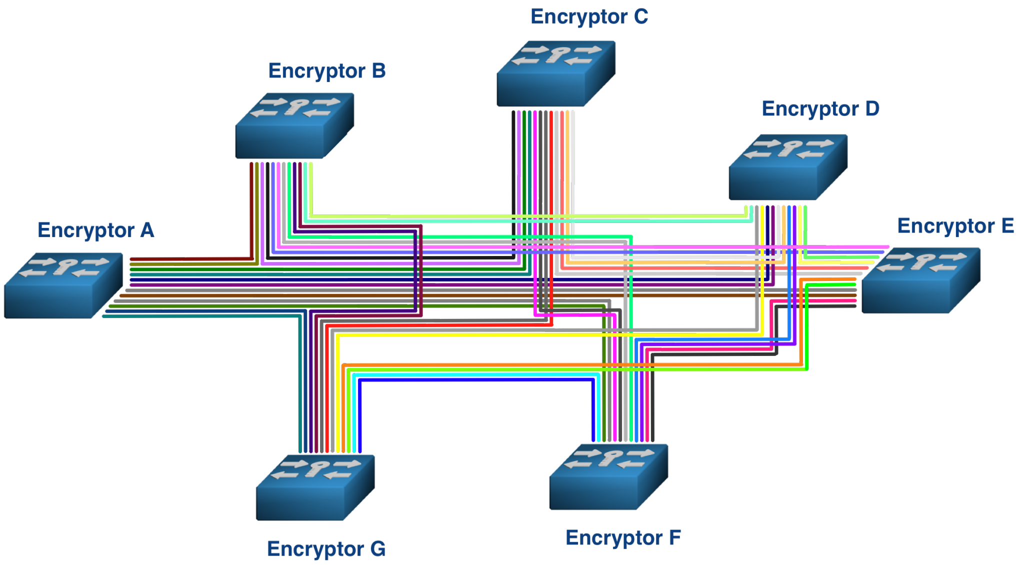
For a pairwise key system point-to-point connections consist of a link whose end-points are defined by the two encryptors A and B. For the encryption of the data flowing from A to B the encryptor uses key AB. In the opposite direction, from B to A, the encryptor uses key BA.

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.



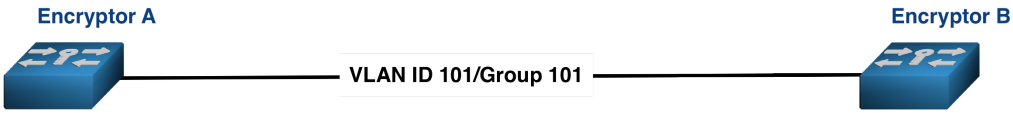
There are four different solution approaches for this problem: (1) Leave multicast and broadcast frames unencrypted, (2) replicate multicast and broadcast frames for every connection and then treat them as unicast frames, (3) add a specialized key system take care of multicast and broadcast frames, and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

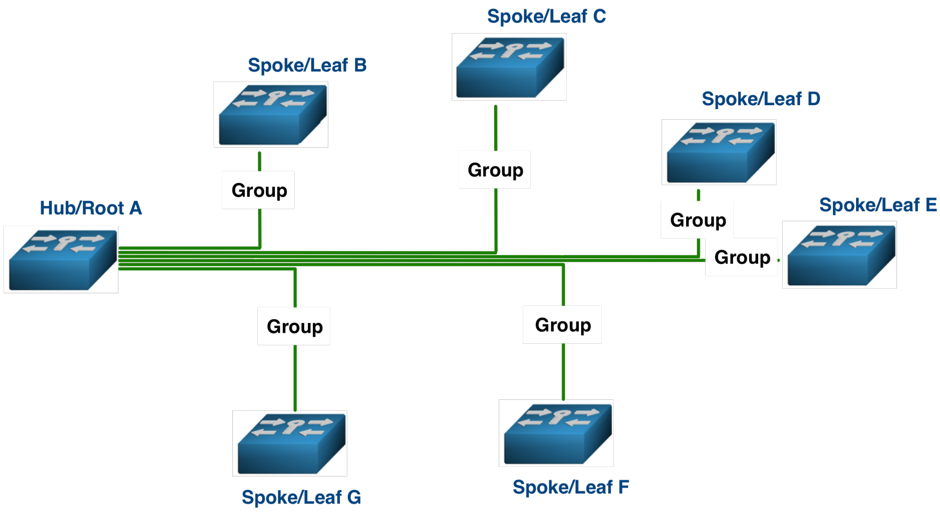
6.5.2. Group Keys

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,

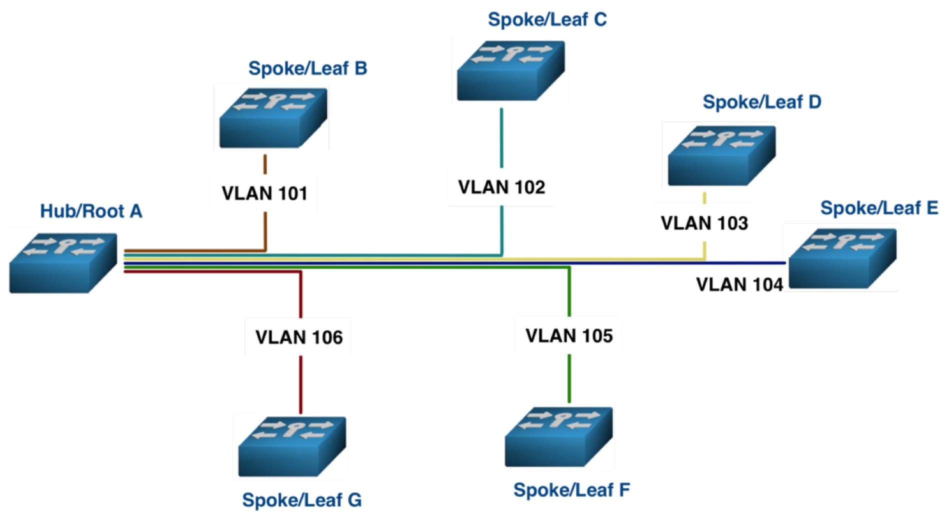
This works for all three basic topologies, starting with point-to-point:



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

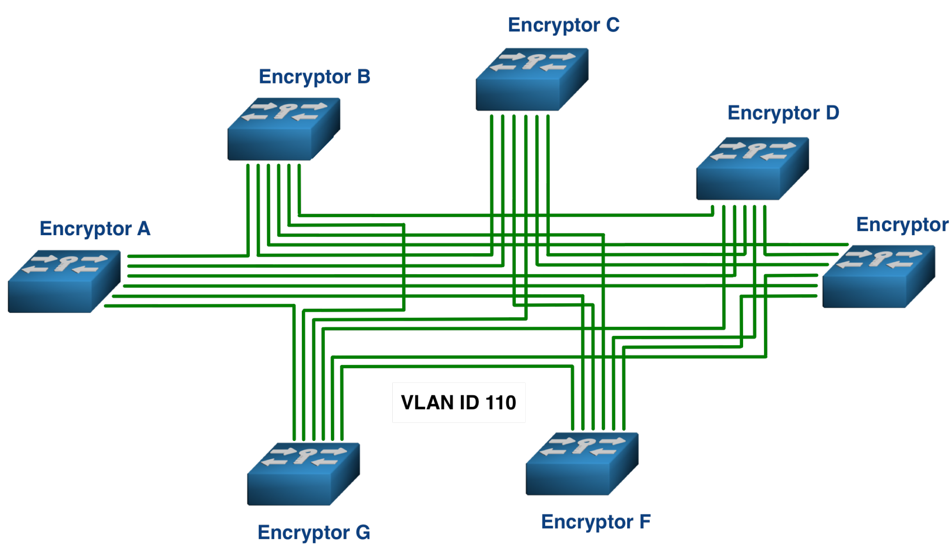


Or each connection between the hub and a spoke is treated as a single group.

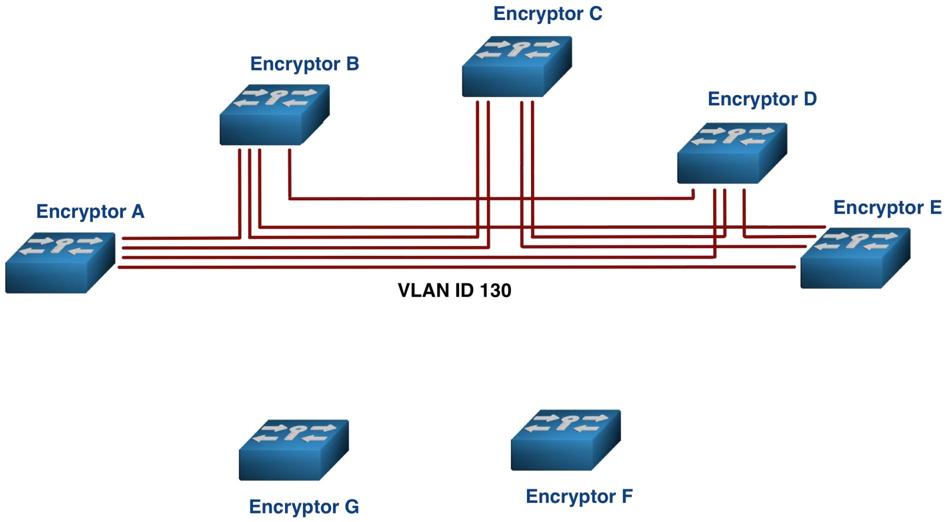


It is also possible to use a mix between the two approaches.

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.

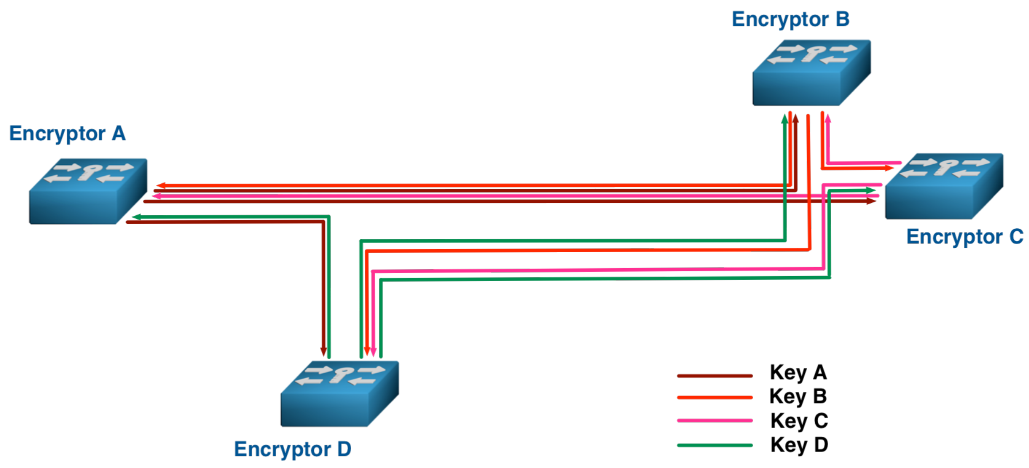


Multipoint connections often are groups that share a common broadcast domain. Within a group all data traffic is encrypted with the same session key. There is no differentiation between unicast, multicast and broadcast frames.

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 encrypion 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 encrpytor, 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/

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 provide 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 by state organizations tend 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, but you can be assured that the device design and development has been under scrutiny from cryptographers, mathematicians and security experts since the beginning. The examination of the final products tends to be rather detailed as well. Such a combined expertise can rarely be found with commercial service providers. The German Bundesamt für Sicherheit in der Informationstechnik has the reputation of being especially demanding for products that are examined and tested following the guidelines of the "IT-Grundschutz" for use by the German government. The technical guidelines published by BSI also tend to be more security-focused and strict compared to some of the NIST requirements. For all certifications, what matters is who examined and tested what where and how and according to which protection profile and guidelines.

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 can hardly be compared as each vendor supports a different feature set on his encyptor 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.

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 pre-condition 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 failover configuration.

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

11. Price and Warranty

11.1. Price

Shown are the list prices. These are now much closer to the actual prices paid than they used to be. Project prices can differ depending on project size. Prices are not necessarily proportional to the functionality and quality of a device.
Some vendors compensate inflated list prices with corresponding discounts, while others work with realistic list prices and correspondingly lower discounts. At the end, it is the price paid that counts and not the discount. The prices are now in a region that facilitates a buy decision. For devices with a full-duplex throughput of 1Gb/s they are now between €13'000 and €20'000, for 10Gb/s full-duplex they are now between €24'000 and €30'000 and for 100Mb/s they are around €6'000. Compact units without redundant power supplies are – depending on platform and vendor – 20-50% below the list prices for 19" appliances with redundant power supplies. A price lower by 50% normally indicates a price at the upper edge of the spread for the 19" appliance. Those prices are for complete and secure systems, including authentication, key management and real-time encryption.
Many vendors do prefer not to see their pricing information published. The pricing spreads shown above do take all the different pricings – published or not - in count.

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 coverage. Different cost structures can account for hidden price differences that can be 10-20%.

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

Michael Braun (atmedia), Mike Churillo (ViaSat), Julian Fay (Senetas), Carsten Fischer (Secunet), Joerg Friedrich (atmedia), Gabi Gerber (Security Interest Group Switzerland/SIGS), Sharon Ginga (Gemalto), Andreas Graubner (Rohde & Schwarz), Harald Herrmann (Rohde & Schwarz), Christoph Hugenschmidt (Inside-IT), Emil Isaakian (ViaSat), Felix Jaggi, Ronald Kuhls (Rohde & Schwarz), Stephan Lehmann, Franjo Majstor, Todd Moore (Gemalto), Ivan Pepelnjak (IPSpace.net), Grégoire Ribordy (ID-Quantique), Kelly Richdale (IDQuantique), David Ristow (Secunet), Peter Rost (Rohde & Schwarz), Gilles Trachsel (IDQuantique), Patrick Trinkler (IDQuantique), Joe Warren (Thales), John Weston (Senetas) and the countless other people, who supported this project in one way or another.

Atmedia

	Virtual Appliance	50/100 compact	1G compact	100M	1G	10G	40G	100G
Line Interface/Supported Line Rates								
							Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps	✔				✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps	✔						✔/QSFP	✔/QSFP28
40 Gbps	✔						✔/QSFP	✔/QSFP28
100 Gbps	✔							✔/QSFP28
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	✔	✔	✔	✔	✔	✔	✔	✔
IP v4/v6	✔	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)								
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios								
Single tenant	✔	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔	✔	✔
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	atmedia

Atmedia

Data Plane Encryption Standard and Processing								
Encryption Standard								
Block Cipher	AES	AES	AES	AES	AES	AES	AES	AES
Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM	GCM	GCM
Alternative Mode of Operation								
Key Length (in bit)	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
store & forward	N/A	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs
Latency MP Mode cut-through	N/A	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs
store & forward	N/A	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs
Encryption Modes								
Native Ethernet Encryption								
Frame Encryption (Bulk - P2P only)	✔	✔	✔	✔	✔	✔	✔	✔
Integrity protection (algorithm)	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
Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8	8
Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	18/26
Ethernet multi-hop support	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
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	unlimited	256	unlimited	256	unlimited	256	unlimited	256
Integrity protection (algorithm)	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
Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 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	✔	✔	✔	✔	✔	✔	✔	✔
Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	✔	✔
Counter length (in bytes)	8	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	18/26	18/26
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	✔
Tunnel (Ethernet over Ethernet)	✔	✔	✔	✔	✔	✔	✔	✔
Max. number of peers	32	32	32	32	32	32	32	32
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	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
Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

Atmedia

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
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)
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	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
Replay protection	✔	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	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 Tunnel Mode								
Mximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	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
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
Counter length (in bytes)	8	8	8	8	8	8	8	8
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66
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	✔	✔	✔	✔	✔	✔	✔	✔
Traffic Masking								
Traffic Flow Security	N/A**	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

Atmedia

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	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
Asymmetric Key Algorithms (Public Key Cryptography)								
RSA								
Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)								
Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:								
NIST	✔	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms								
SHA-2 Key length	512	512	512	512	512	512	512	512
CBC-MAC-GCM Key length	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)
Key length	256	256	256	256	256	256	256	256
Asymmetric Signature: Certificate	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)
Key lenght	512	512	512	512	512	512	512	512
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****
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*****
Master Key (KEK) Exchange Protocol	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
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
Session Key (DEK) Exchange Protocol	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

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Atmedia

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
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
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
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)	✔	✔	✔	✔	✔	✔	✔	✔

Atmedia

Network Support								
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE	✔	✔	✔	✔	✔	✔	✔	✔
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
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
TLS								
Proprietary	✔	✔	✔	✔	✔	✔	✔	✔
Remote Monitoring (SNMP)	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
Number of external encrypted Ethernet ports	unrestricted	1	1	1	1	1	1-4	1-4
Physical Device Access	N/A	back	back	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
MTBF	N/A	> 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
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	N/A	25s	25s	25s	25s	25s	25s	25s
Warm boot until operational	N/A	27s	27s	27s	27s	27s	27s	27s

*****BSI VS-NfD, NATO restricted and EU Restrint planned/in preparation

Atmedia

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
Number of roles	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
Certificate Creation	optional	optional	optional	optional	optional	optional	optional	optional
Certificate Management	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
Per external Key Server (in €); optional, no requirement	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
11-25 encryptors	included	included	included	included	included	included	included	included
26-50 encryptors	included	included	included	included	included	included	included	included
51+ encryptors	included	included	included	included	included	included	included	included
Warranty Period (months)	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
Software updates and upgrades	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

Gemalto

	Safenet CN4010	Safenet CN4020	Safenet CN6010	Safenet CN6100	Safenet CN8000	Safenet CN9100	Safenet CN9120
Line Interface/Supported Line Rates							
10 Mbs	✔/RJ45	✔/SFP	✔/RJ45/SFP				
100 Mps	✔/RJ45	✔/SFP	✔/RJ45/SFP				
1 Gbps	✔/RJ45	✔/SFP	✔/RJ45/SFP	✔/SFP	✔/SFP+		
10 Gbps				✔/SFP	✔/SFP+		
25Gps							
40 Gbps					✔/SFP+		
100 Gbps					✔/SFP+ up to 10 cards at up to 10G each	✔/CFP-4	✔/QSFP-28
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)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
TCP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
UDP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	*	*	*	*	✔/one tenant per port	*	
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/IDQuantique	Senetas/Senetas	Senetas/Senetas
Key Management	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas

* IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency.
* Multi-tenancy support based on certificates. Requires common trust domain of CAs.

Gemalto

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	CTR	CTR	
Alternative Mode of Operation	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	GCM (Roadmap Q4 2017)	GCM (Roadmap Q4 2017)	
Key Length (in bit)	128/256	128/256	128/256	128/256	128/256	128/256	128/256	
Processing Method								
cut-through	✔	✔	✔	✔	✔			
store&forward	*	*	*	*	*	✔	✔	
Encryption Hardware								
FPGA	✔	✔	✔	✔	✔	✔	✔	
ASIC								
CPU								
Latency								
Latency P2P Mode cut-through	<10μs (@1Gbps)	<10μs (@1Gbps)	<10μs	<5μs	<5μs			
store & forward	*	*	*	*	*	<2μs	<2μs	
Latency MP Mode cut-through	<10μs (@1Gbps)	<10μs (@1Gbps)	<10μs	<5μs	<5μs			
store & forward	*	*	*	*	*	<2μs	<2μs	
Encryption Modes								
Native Ethernet Encryption								
Frame Encryption (Bulk - P2P only)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
Authentication length (bytes)	16	16	16	16				
Replay protection	✔	✔	✔	✔				
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
Counter length (in bytes)	5	5	5	5				
Frame overhead (unauthenticated encryption)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)				
Frame overhead (authenticated encryption)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
Ethernet multi-hop support	✔	✔	✔	✔				
Transport (Payload only)	✔	✔	✔	✔	✔	✔	✔	
Max. number of peers	512	512	512	512	512	512	512	
Max. number of MAC Addresses	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	limitation only in MAC mod
Max. number of VLAN IDs	256	256	256	512	512	512	512	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	*GCM (Roadmap Q4 2017)	*GCM (Roadmap Q4 2017)	
Authentication length (bytes)	16	16	16	16	16	16	16	
Replay protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	
Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
Ethertype mutation	✔	✔	✔	✔	✔	✔	✔	
Counter length (in bytes)	5	5	5	5	5	5	5	
Frame overhead unauthenticated encryption	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	8 (CTR)	8 (CTR)	
Frame overhead authenticated encryption (AE)	24	24	24	24	24	24*	24*	*GCM (Roadmap Q4 2017)
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)	*	*	*	*	*	* Roadmap Q4 2017	* Roadmap Q4 2017	
Max. number of peers	2	2	2	2				
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited				
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited				
Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
Authentication length (bytes)	16	16	16	16				
Replay protection	✔	✔	✔	✔				
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
Counter length (in bytes)	5	5	5	5				
Frame overhead unauthenticated encryption	8 (CTR)	8 (CTR)	8 (CTR)	8 (CTR)				
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
Ethernet multi-hop support	✔	✔	✔	✔				

* except for CN9100/CN9120 store & forward only in combination with TRANSEC and limited to P2P. Frame mode, tunnel mode and EoIP only when using TRANSEC. Frame mode not native. Additional overhead and latency.

Gemalto

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported transmission protocols (UDP/TCP)	UDP/TCP	UDP/TCP	UDP/TCP	UDP/TCP			
Max. number of peers	2	2	2	2			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited			
Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
Authentication length (bytes)	16	16	16	16			
Replay protection	✔	✔	✔	✔			
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
Counter length (in bytes)	5	5	5	5			
Frame overhead unauthenticated encryption	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38			
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)			
Ethernet multi-hop support	✔	✔	✔	✔			
Native IP Encryption							
Supported IP versions							
IPv4							
IPv6							
Supported transmission protocols							
TCP							
UDP							
Transport/Tunnel 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)							
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							
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔		Roadmap Q4 2017	Roadmap Q4 2017

Gemalto

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	✔	✔	✔	✔	✔/QRNG	✔QRNG	✔/QRNG
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)							
RSA							
Key length	2048	2048	2048	2048	2048	2048	2048
Elliptic Curve Cryptography (ECC)							
Key length	512	512	512	512	512	512	512
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)							
Maximum number of PSKs per encryptor							
Key length							
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	x.509	x.509	x.509
Maximum number of certificates per encryptor	64	64	64	64	64	64	64
Key length	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)
Ad-hoc authentication of peers (manual)							
Signature key protocol	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA
Master Key (KEK) Exchange Protocol	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	1440	1440	1440	1440	1440	1440	1440
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications
Session Key (DEK) Exchange Protocol	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

Key System	Gemalto						
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)	✔	✔	✔	✔	✔	✔	✔

Gemalto

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE							
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)	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW
TLS							
Proprietary							
Remote Monitoring (SNMP)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3
Logs							
Event Log (local)	✔	✔	✔	✔	✔	✔	✔
Audit Log (local)	✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔
Unit							
Height in 19" Rack	Desktop	Desktop	1U	1U	4U	1U	1U
Number of external encrypted Ethernet ports	1	1	1	1	1-10	1	1
Physical Device Access	back	back	front	front	front	front	front
Redundant Power Supply			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017
MTBF	> 200.000h	> 200.000h	> 200.000h	> 200.000h	> 100.000h	> 200.000h	> 200.000h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+	FIPS140-2 L3/ CC EAL2+ in progress	*
Safety Approvals	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000 ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS
Boot Time							
Cold boot until operational (P2P)	65s	65s	65s	65s	65s	65s	65s
Warm boot until operational (P2P)	80s	80s	80s	80s	80s	80s	80s

* For CN 9100 CC EAL2+ in progress, for CN 9120, FIPS 140-2 L3 and CC EAL2+ planned. For both: UC APL and NATO planned

Gemalto

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
	Number of roles	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)
	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 €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement, starting price		on request	on request	on request	on request	on request	on request	on request
Required Management Software		CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included
Optional SMC Sofware	1-4 encryptors	free	free	free	free	free	free	free
	5-10 encryptors	on request	on request	on request	on request	on request	on request	on request
	11-20 encryptors	on request	on request	on request	on request	on request	on request	on request
	unlimited	on request	on request	on request	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		15%	15%	15%	15%	15%	15%	15%%

* Additionally available: Premium support (24x7 support, Advance RMA) with Plus Maintenance

Idquantique

	Centauris CN4010	Centauris CN4020	Centauris CN6010	Centauris CN6100	Centauris CN8000	Centauris CN9100	Centauris CN9120
Line Interface/Supported Line Rates							
10 Mbs	✔/RJ45	✔/SFP	✔/RJ45/SFP				
100 Mps	✔/RJ45	✔/SFP	✔/RJ45/SFP				
1 Gbps	✔/RJ45	✔/SFP	✔/RJ45/SFP	✔/SFP	✔/SFP+		
10 Gbps				✔/SFP	✔/SFP+		
25Gps							
40 Gbps					✔/SFP+		
100 Gbps					✔/SFP+	✔/CFP-4	✔/QSFP-28
					up to 10 cards at up to 10G each		
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)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
TCP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
UDP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	*	*	*	*	✔/one tenant per port	*	
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/IDQuantique	Senetas/Senetas	Senetas/Senetas
Key Management	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas

* IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency.
* Multi-tenancy support based on certificates. Requires common trust domain of multiple CAs or use of a single CA

Idquantique

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	CTR	CTR	
Alternative Mode of Operation	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	GCM (Roadmap Q4 2017)	GCM (Roadmap Q4 2017)	
Key Length (in bit)	128/256	128/256	128/256	128/256	128/256	128/256	128/256	
Processing Method								
cut-through	✔	✔	✔	✔	✔			
store&forward	*	*	*	*	*	✔	✔	
Encryption Hardware								
FPGA	✔	✔	✔	✔	✔	✔	✔	
ASIC								
CPU								
Latency								
Latency P2P Mode cut-through	<10μs (@1Gbps)	<10μs (@1Gbps)	<10μs	<5μs	<5μs			
store & forward	*	*	*	*	*	<2μs	<2μs	
Latency MP Mode cut-through	<10μs (@1Gbps)	<10μs (@1Gbps)	<10μs	<5μs	<5μs			
store & forward	*	*	*	*	*	<2μs	<2μs	
Encryption Modes								
Native Ethernet Encryption								
Frame Encryption (Bulk - P2P only)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
Authentication length (bytes)	16	16	16	16				
Replay protection	✔	✔	✔	✔				
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
Counter length (in bytes)	5	5	5	5				
Frame overhead (unauthenticated encryption)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)				
Frame overhead (authenticated encryption)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
Ethernet multi-hop support	✔	✔	✔	✔				
Transport (Payload only)	✔	✔	✔	✔	✔	✔	✔	
Max. number of peers	512	512	512	512	512	512	512	
Max. number of MAC Addresses	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	limitation only in MAC mode
Max. number of VLAN IDs	256	256	256	512	512	512	512	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	*GCM (Roadmap Q4 2017)	*GCM (Roadmap Q4 2017)	
Authentication length (bytes)	16	16	16	16	16	16	16	
Replay protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	
Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
Ethertype mutation	✔	✔	✔	✔	✔	✔	✔	
Counter length (in bytes)	5	5	5	5	5	5	5	
Frame overhead unauthenticated encryption	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	8 (CTR)	8 (CTR)	
Frame overhead authenticated encryption (AE)	24	24	24	24	24	24*	24*	*GCM (Roadmap Q4 2017)
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)	*	*	*	*	*	* Roadmap Q4 2017	* Roadmap Q4 2017	
Max. number of peers	2	2	2	2				
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited				
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited				
Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
Authentication length (bytes)	16	16	16	16				
Replay protection	✔	✔	✔	✔				
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
Counter length (in bytes)	5	5	5	5				
Frame overhead unauthenticated encryption	8 (CTR)	8 (CTR)	8 (CTR)	8 (CTR)				
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
Ethernet multi-hop support	✔	✔	✔	✔				

* except for CN9100/CN9120 store & forward only in combination with TRANSEC and limited to P2P. Frame mode, tunnel mode and EoIP only when using TRANSEC. Frame mode not native. Additional overhead and latency.

Idquantique

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported transmission protocols (UDP/TCP)	UDP/TCP	UDP/TCP	UDP/TCP	UDP/TCP			
Max. number of peers	2	2	2	2			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited			
Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
Authentication length (bytes)	16	16	16	16			
Replay protection	✔	✔	✔	✔			
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
Counter length (in bytes)	5	5	5	5			
Frame overhead unauthenticated encryption	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38			
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)			
Ethernet multi-hop support	✔	✔	✔	✔			
Native IP Encryption							
Supported IP versions							
IPv4							
IPv6							
Supported transmission protocols							
TCP							
UDP							
Transport/Tunnel 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)							
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							
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔		Roadmap Q4 2017	Roadmap Q4 2017

* EoIP only when using TRANSEC. Limited to P2P. Additional overhead and latency.

	Idquantique						
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	✔	✔	✔	✔	✔/QRNG	✔QRNG	✔/QRNG
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)							
RSA							
Key length	2048	2048	2048	2048	2048	2048	2048
Elliptic Curve Cryptography (ECC)							
Key length	512	512	512	512	512	512	512
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)							
Maximum number of PSKs per encryptor							
Key length							
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	x.509	x.509	x.509
Maximum number of certificates per encryptor	64	64	64	64	64	64	64
Key length	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)
Ad-hoc authentication of peers (manual)							
Signature key protocol	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA
Master Key (KEK) Exchange Protocol	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	1440	1440	1440	1440	1440	1440	1440
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications
Session Key (DEK) Exchange Protocol	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

Idquantique

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)	✔	✔	✔	✔	✔	✔	✔

Idquantique

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE							
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)	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW
TLS							
Proprietary							
Remote Monitoring (SNMP)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3
Logs							
Event Log (local)	✔	✔	✔	✔	✔	✔	✔
Audit Log (local)	✔	✔	✔	✔	✔	✔	✔
Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔
Unit							
Height in 19" Rack	Desktop	Desktop	1U	1U	4U	1U	1U
Number of external encrypted Ethernet ports	1	1	1	1	1-10	1	1
Physical Device Access	back	back	front	front	front	front	front
Redundant Power Supply			✔	✔	✔	✔	✔
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔
High Availability functionality (two-node cluster)	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017
MTBF	> 200.000h	> 200.000h	> 200.000h	> 200.000h	> 100.000h	> 200.000h	> 200.000h
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Security Approvals	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+	FIPS140-2 L3/ CC EAL2+ in progress	*
Safety Approvals	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000 ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS
Boot Time							
Cold boot until operational (P2P)	65s	65s	65s	65s	65s	65s	65s
Warm boot until operational (P2P)	80s	80s	80s	80s	80s	80s	80s

* For CN 9100 CC EAL2+ in progress, for CN 9120, FIPS 140-2 L3 and CC EAL2+ planned. For both: UC APL and NATO planned

Idquantique

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
	Number of roles	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)
	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 €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement, starting price		on request	on request	on request	on request	on request	on request	on request
Required Management Software		CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included
Optional SMC Sofware	1-4 encryptors	free	free	free	free	free	free	free
	5-10 encryptors	on request	on request	on request	on request	on request	on request	on request
	11-20 encryptors	on request	on request	on request	on request	on request	on request	on request
	unlimited	on request	on request	on request	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		10%	10%	10%	10%	10%	10%	10%

* Additionally available: Premium support (24x7 support, Advance RMA) with Plus Maintenance

Rohde & Schwarz Cybersecurity

	SITLine ETH50	SITLine ETH4G	SITLine ETH10G	SITLine ETH40G	
Line Interface/Supported Line Rates					
10 Mbs	✔/RJ45	✔/4xRJ45/4xSFP	✔/4xRJ45/4xSFP+		
100 Mps	✔/RJ45	✔/4xRJ45/4xSFP	✔/4xRJ45/4xSFP+		
1 Gbps		✔/4xRJ45/4xSFP	✔/4xRJ45/4xSFP+		
10 Gbps		✔/(license upgrade)	✔/4xRJ45/4xSFP+	✔/4xRJ45/4xSFP+	
25Gps					
40 Gbps				✔/QSFP	on request
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					supported by SITline IP Roadmap Q3 2017
IPv4/IPv6					supported by SITline IP Roadmap Q3 2017
Supported Networks (Transport of Encrypted Frame)					
Ethernet (native)	✔	✔	✔	✔	
MPLS (EoMPLS)	✔	✔	✔	✔	
IPv4/IPv6					supported by SITline IP Roadmap Q3 2017
TCP					supported by SITline IP Roadmap Q3 2017
UDP					supported by SITline IP Roadmap Q3 2017
Supported Usage Scenarios					
Single tenant	✔	✔	✔	✔	
Multi-tenant					
Self-managed	✔	✔	✔	✔	
Managed encryption service	✔	✔	✔	✔	
Managed security service	✔	✔	✔	✔	separate network and security management (NMS, SMS)
Platform					
Platform used					
Mainboard/Firmware	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	
Key Management	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	

Rohde & Schwarz Cybersecurity

Data Plane Encryption Standard and Processing				
Encryption Standard				
Block Cipher	AES	AES	AES	AES
Preferred Mode of Operation	GCM	GCM	GCM	GCM
Alternative Mode of Operation	CFB	CFB	CFB	CFB
Key Length (in bit)	256	256	256	256
Processing Method				
cut-through		✔	✔	✔
store&forward	✔	✔	✔	✔
Encryption Hardware				
FPGA	✔	✔	✔	✔
ASIC				
CPU				
Latency				
Latency P2P Mode cut-through	N/A	5µs	<3µs	<3µs
store & forward	*	*	*	*
Latency MP Mode cut-through	N/A	5µs	<3µs	<3µs
store & forward	*	*	*	*
Encryption Modes				
Native Ethernet Encryption				
Frame Encryption (Bulk - P2P only)		✔	✔	✔
Integrity protection (algorithm)		GCM	GCM	GCM
Authentication length (bytes)		8-16	8-16	8-16
Replay protection		✔	✔	✔
Variable replay window (size)		3 frames per priority	3 frames per priority	3 frames per priority
Counter length (in bytes)		5	5	5
Frame overhead (unauthenticated encryption)		0 (CFB), 5 (CTR)	0 (CFB), 5 (CTR)	0 (CFB), 5 (CTR)
Frame overhead (authenticated encryption)		13-21	13-21	13-21
Transport (Payload only)	✔	✔	✔	✔
Max. number of peers	250	4000	4000	4000
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	250	4000	4000	4000
Integrity protection (algorithm)	GCM	GCM	GCM	GCM
Authentication length (bytes)	8-16	8-16	8-16	8-16
Replay protection	✔	✔	✔	✔
Variable replay window (size)	3 frames per priority	3 frames per priority	3 frames per priority	3 frames per priority
Definable encryption offset (fixed)				
Variable encryption offset	✔	✔	✔	✔
Adaptive encryption offset based on frame content	✔	✔	✔	✔
Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔
Counter length (in bytes)	5	5	5	5
Frame overhead unauthenticated encryption	5 (PP)/ 10 (MP)	5 (PP)/ 10 (MP)	5 (PP)/ 10 (MP)	5 (PP)/ 10 (MP)
Frame overhead authenticated encryption (AE)	13-21 (PP), 18-26 (MP)	13-21 (PP), 18-26 (MP)	13-21 (PP), 18-26 (MP)	13-21 (PP), 18-26 (MP)
Ethernet multi-hop support	✔	✔	✔	✔
Tunnel (Ethernet over Ethernet)	✔	✔	✔	✔
Max. number of peers	250	4000	4000	4000
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	250	4000	4000	4000
Integrity protection (algorithm)	GCM	GCM	GCM	GCM
Authentication length (bytes)	8-16	8-16	8-16	8-16
Replay protection	✔	✔	✔	✔
Variable replay window (size)	3 frames per priority	3 frames per priority	3 frames per priority	3 frames per priority
Counter length (in bytes)	5	5	5	5
Frame overhead unauthenticated encryption	20	20	20	20
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 (P2P), 28-36 (MP)
Ethernet multi-hop support	✔	✔	✔	✔

* dependent on packet size/bandwidth

tunnel in multipoint mode only replaces destination address

Rohde & Schwarz Cybersecurity

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)					
Replay protection					
Variable replay window (size)					
Counter length (in bytes)					
Frame overhead unauthenticated encryption					
Frame overhead authenticated encryption (AE)					
Ethernet multi-hop support					
Native IP Encryption					
Supported IP versions					
IPv4					supported by SITline IP Roadmap Q3 2017
IPv6					supported by SITline IP Roadmap Q3 2017
Supported transmission protocols					
TCP					supported by SITline IP Roadmap Q3 2017
UDP					supported by SITline IP Roadmap Q3 2017
Transport/Tunnel Mode					supported by SITline IP Roadmap Q3 2017
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)					
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					
Traffic Masking					
Traffic Flow Security					

Rohde & Schwarz Cybersecurity

Auto-discovery					
Auto-discovery of network encryptors	✔	✔	✔	✔	
Auto-discovery of key servers	✔	✔	✔	✔	
Auto-discovery of VLANs	✔	✔	✔	✔	Automatische Partnersuche über 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	N/A	N/A	N/A	N/A	
Autonomous operation	✔	✔	✔	✔	
Key Management					
Key Generation and Storage					
Hardware Random Number Generation	✔ (PTG-3)	✔ (PTG-3)	✔ (PTG-3)	✔ (PTG-3)	
Tamper Security Key Storage (tamper-evident or tamper-proof)	TE/TP	TE/TP	TE/TP	TE/TP	
Asymmetric Key Algorithms (Public Key Cryptography)					
RSA					
Key length	2048	2048	2048	2048	
Elliptic Curve Cryptography (ECC)					
Key length	257	257	257	257	
Supported Curves:					
NIST					
Brainpool					
Custom Curves	✔	✔	✔	✔	
Hash Algorithms					
SHA-2 Key length	256	256	256	256	
Device Authentication					
Symmetric Signature: Pre-shared Key (PSK)					
Maximum number of PSKs per encryptor					
Key length					
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	
Maximum number of certificates per encryptor	1	1	1	1	
Key lenght	257	257	257	257	
Ad-hoc authentication of peers (manual)	✔	✔	✔	✔	
Signature key protocol	ECDSA	ECDSA	ECDSA	ECDSA	
Key Agreement and Key Exchange					
Master Key (KEK) Agreement	DH-ECKAS	DH-ECKAS	DH-ECKAS	DH-ECKAS	
Master Key (KEK) Exchange Protocol	ECDH	ECDH	ECDH	ECDH	
Automatic Change of Master Key	✔	✔	✔	✔	
Minimum suggested Time Interval for Master Key Change (min)	360	360	360	360	
Separate Master Key (KEK) per site	✔	✔	✔	✔	
Separate Master Key (KEK) per group					
Session Key (DEK) Exchange Agreement	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	
Session Key (DEK) Exchange Protocol	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	Rohde & Schwarz	
Automatic Change of Session Keys	✔	✔	✔	✔	
Minimum Time Interval for Session Key Change (min)	1	1	1	1	

Key System	Rohde & Schwarz Cybersecurity			
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	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)				

Rohde & Schwarz Cybersecurity

Network Support					
Bump in the Wire deployment	✔	✔	✔	✔	
Jumbo Frame Support	✔	✔	✔	✔	bis 16000 Bytes
Ethernet Flow Control via PAUSE	✔	✔	✔	✔	
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)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	
Logs					
Event Log (local)	✔	✔	✔	✔	
Audit Log (local)	✔	✔	✔	✔	
Syslog Support (Server)	✔	✔	✔	✔	
Unit					
Height in 19" Rack	1U (1/2 19" width)	1	1	1	
Number of external encrypted Ethernet ports	1	1 or 4	1 or 4	1 or 4	
Physical Device Access	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	
MTBF	350000h	170000h	170000h	170000h	
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	
Security Approvals	BSI VS-NfD, EU restreint	BSI VS-NfD, EU restreint	BSI VS-NfD, EU restreint, **CC EAL4+	BSI VS-NfD, EU restreint, **CC EAL4+	CC EAL 4+ pending
Safety Approvals	CE, ROHS	CE, ROHS	CE, ROHS	CE, ROHS	
Boot Time					
Cold boot until operational (P2P)	60s	40s	40s	40s	
Warm boot until operational (P2P)	60s	40s	40s	40s	

Rohde & Schwarz Cybersecurity

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	
	Number of roles	8	8	8	8	customizable 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	✔	✔	✔	✔	via key management
	Key assignment	✔	✔	✔	✔	
	Fail-over configuration	✔	✔	✔	✔	

Price

List Price Encryption Unit (in €)		on request	on request	on request	on request
Per external Key Server (in €)					
Required Management Software		on request	on request	on request	on request
	2-10 encryptors	on request	on request	on request	on request
	11-25 encryptors	on request	on request	on request	on request
	26-50 encryptors	on request	on request	on request	on request
	51+ encryptors	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	3%	3%	3%	3%
	Software updates and upgrades	3%	3%	3%	3%
Warranty Extension (per year)		5%	5%	5%	5%

Secunet

	50M compact	100M	1G	10G	40G	100G
Line Interface/Supported Line Rates						
					Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps			✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps					✔/QSFP	✔/QSFP28
40 Gbps					✔/QSFP	✔/QSFP28
100 Gbps						✔/QSFP28
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	✔	✔	✔	✔	✔	✔
IP v4/v6	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)						
Ethernet (native)	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios						
Single tenant	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔
Self-managed	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔
Platform						
Platform used						
Mainboard/Firmware	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia/atmedia	atmedia
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Secunet

Data Plane Encryption Standard and Processing						
Encryption Standard						
Block Cipher	AES	AES	AES	AES	AES	AES
Preferred Mode of Operation	GCM	GCM	GCM	GCM	GCM	GCM
Alternative Mode of Operation						
Key Length (in bit)	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	<8µs	<4µs	<4µs	<2µs
store & forward	<48µs	<48µs	<9µs	<4µs	<4µs	<2µs
Latency MP Mode cut-through	<42µs	<42µs	<8µs	<4µs	<4µs	<2µs
store & forward	<48µs	<48µs	<9µs	<4µs	<4µs	<2µs

Encryption Modes						
Native Ethernet Encryption						
Frame Encryption (Bulk - P2P only)	✔	✔	✔	✔	✔	✔
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16
Replay protection	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8
Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26
Ethernet multi-hop support	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
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	256	256	unlimited	256	unlimited	256
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16
Replay protection	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 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	✔	✔	✔	✔	✔	✔
Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔
Counter length (in bytes)	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔
Tunnel (Ethernet over Ethernet)	✔	✔	✔	✔	✔	✔
Max. number of peers	32	32	32	32	32	32
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16
Replay protection	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔

*IMIX=100%

Secunet

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
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)
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	8/16	8/16	8/16	8/16	8/16	8/16
Replay protection	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Registered Ethertype	✔	✔	✔	✔	✔	✔
Counter length (in bytes)	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	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 Tunnel Mode						
Mximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of IP addresses	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Maximum number of multicast groups	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	GCM
Authentication length (bytes)	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
Counter length (in bytes)	8	8	8	8	8	8
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66
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	✔	✔	✔	✔	✔	✔
Traffic Masking						
Traffic Flow Security	✔	✔	✔	✔	✔	✔

*IMIX=100%

**TFS mode only secure based on ASIC or FPGA

Secunet

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	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)						
RSA						
Key length	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)						
Key length	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:						
NIST	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔
Hash Algorithms						
SHA-2 Key length	512	512	512	512	512	512
CBC-MAC-GCM Key length	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)
Key length	256	256	256	256	256	256
Asymmetric Signature: Certificate	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)
Key lenght	512	512	512	512	512	512
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****
Key Agreement and Key Exchange						
Master Key (KEK) Agreement	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****	ECKAS-DH*****
Master Key (KEK) Exchange Protocol	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
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia
Session Key (DEK) Exchange Protocol	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

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Secunet

Key System						
Point-to-Point Key System						
Supported key system						
Pairwise	✔	✔	✔	✔	✔	✔
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
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
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)	✔	✔	✔	✔	✔	✔

Secunet

Network Support						
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE	✔	✔	✔	✔	✔	✔
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
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
TLS						
Proprietary	✔	✔	✔	✔	✔	✔
Remote Monitoring (SNMP)	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
Number of external encrypted Ethernet ports	1	1	1	1	1-4	1-4
Physical Device Access	back	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
MTBF	> 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
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	25s	25s	25s	25s	25s	25s
Warm boot until operational	27s	27s	27s	27s	27s	27s

*****BSI VS-NfD, NATO restricted and EU Restrint planned/in preparation

Secunet

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
	Number of roles	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
	Certificate Creation	optional	optional	optional	optional	optional	optional
	Certificate Management	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
Per external Key Server (in €); optional, no requirement		on request	on request	on request	on request	on request	on request
Required Management Software (SINA Software optional)							
	2-10 encryptors	included	included	included	included	included	included
	11-25 encryptors	included	included	included	included	included	included
	26-50 encryptors	included	included	included	included	included	included
	51+ encryptors	included	included	included	included	included	included
Warranty Period (months)		36	36	36	36	36	36
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

Securosys

	Centurion 50/100 compact	Centurion 1G compact	Centurion 100M	Centurion 1G	Centurion 10G	Centurion 40G	Centurion 100G
Line Interface/Supported Line Rates							
						Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps				✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps						✔/QSFP	✔/QSFP28
40 Gbps						✔/QSFP	✔/QSFP28
100 Gbps							✔/QSFP28
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	✔	✔	✔	✔	✔	✔	✔
IP v4/v6	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔	✔
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
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Securosys

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	<8μs	<42μs	<8μs	<4μs	<4μs	<2μs
store & forward	<48μs	<9μs	<48μs	<9μs	<4μs	<4μs	<2μs
Latency MP Mode cut-through	<42μs	<8μs	<42μs	<8μs	<4μs	<4μs	<2μs
store & forward	<48μs	<9μs	<48μs	<9μs	<4μs	<4μs	<2μs
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
Replay protection	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8
Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	18/26
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	256	unlimited	256	unlimited	256	unlimited	256
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
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	✔	✔	✔	✔	✔	✔	✔
Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	✔
Counter length (in bytes)	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	18/26
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
Replay protection	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

Securosys

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)	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 Tunnel Mode							
Maximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
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)	8	8	8	8	8	8	8
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66
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	✔	✔	✔	✔	✔	✔	✔
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

**TFS mode only secure based on ASIC or FPGA

Securosys

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	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)							
Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
CBC-MAC-GCM Key length	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
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
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

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Key System	Securosys						
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)	✔	✔	✔	✔	✔	✔	✔

Securosys

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE	✔	✔	✔	✔	✔	✔	✔
Ethernet Fragmentation/Defragmentation	✔	✔	✔	✔	✔	✔	✔
Point-to-Point	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint	✔	✔	✔	✔	✔	✔	✔
Multipoint	✔	✔	✔	✔	✔	✔	✔
Dead Peer Detection	✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through	N/A	N/A	N/A	✔	✔	✔	✔
Link Loss Carry Forward	✔	✔	✔	✔	✔	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	1	1-4	1-4
Physical Device Access	back	back	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		*****	*****	*****	*****	*****	*****
Safety Approvals	EN55032 Class B, FCC Part 15 Class B, ROHS						
Boot Time							
Cold boot until operational	25s	25s	25s	25s	25s	25s	25s
Warm boot until operational	27s	27s	27s	27s	27s	27s	27s

***** Products using the same platform have BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL) approval

Securosys

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
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)	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
Warranty Extension (per year)	on request	on request	on request	on request	on request	on request	on request

Senetas

	CN4010	CN4020	CN6010	CN6100	CN8000	CN9100	CN9120
Line Interface/Supported Line Rates							
10 Mbs	✔/RJ45	✔/SFP	✔/RJ45/SFP				
100 Mps	✔/RJ45	✔/SFP	✔/RJ45/SFP				
1 Gbps	✔/RJ45	✔/SFP	✔/RJ45/SFP	✔/SFP	✔/SFP+		
10 Gbps				✔/SFP	✔/SFP+		
25Gps							
40 Gbps					✔/SFP+		
100 Gbps					✔/SFP+	✔/CFP-4	✔/QSFP-28
					up to 10 cards at up to 10G each		
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)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6							
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
TCP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
UDP	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	*	*	*	*	✔/one tenant per port	*	
Self-managed	✔	✔	✔	✔	✔	✔	✔
Managed encryption service	✔	✔	✔	✔	✔	✔	✔
Managed security service	✔	✔	✔	✔	✔	✔	✔
Platform							
Platform used							
Mainboard/Firmware	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/Senetas	Senetas/IDQuantique	Senetas/Senetas	Senetas/Senetas
Key Management	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas

* IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency.
* Multi-tenancy support based on certificates. Requires common trust domain of multiple CAs or use of a single CA

Senetas

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	CTR	CTR	
Alternative Mode of Operation	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	CFB/CTR	GCM (Roadmap Q4 2017)	GCM (Roadmap Q4 2017)	
Key Length (in bit)	128/256	128/256	128/256	128/256	128/256	128/256	128/256	
Processing Method								
cut-through	✔	✔	✔	✔	✔			
store&forward	*	*	*	*	*	✔	✔	
Encryption Hardware								
FPGA	✔	✔	✔	✔	✔	✔	✔	
ASIC								
CPU								
Latency								
Latency P2P Mode cut-through	<10μs (@1Gbps)	<10μs (@1Gbps)	<10μs	<5μs	<5μs			
store & forward	*	*	*	*	*	<2μs	<2μs	
Latency MP Mode cut-through	<10μs (@1Gbps)	<10μs (@1Gbps)	<10μs	<5μs	<5μs			
store & forward	*	*	*	*	*	<2μs	<2μs	
Encryption Modes								
Native Ethernet Encryption								
Frame Encryption (Bulk - P2P only)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
Authentication length (bytes)	16	16	16	16				
Replay protection	✔	✔	✔	✔				
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
Counter length (in bytes)	5	5	5	5				
Frame overhead (unauthenticated encryption)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)	8 (CTR) + tunnel (min 18 bytes)				
Frame overhead (authenticated encryption)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
Ethernet multi-hop support	✔	✔	✔	✔				
Transport (Payload only)	✔	✔	✔	✔	✔	✔	✔	
Max. number of peers	512	512	512	512	512	512	512	
Max. number of MAC Addresses	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	4000/unlimited	limitation only in MAC mode
Max. number of VLAN IDs	256	256	256	512	512	512	512	
Integrity protection (algorithm)	GCM	GCM	GCM	GCM	GCM	*GCM (Roadmap Q4 2017)	*GCM (Roadmap Q4 2017)	
Authentication length (bytes)	16	16	16	16	16	16	16	
Replay protection	✔	✔	✔	✔	✔	✔	✔	
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	256 frames	
Definable encryption offset (fixed)	✔	✔	✔	✔	✔	✔	✔	
Variable encryption offset	✔	✔	✔	✔	✔	✔	✔	
Adaptive encryption offset based on frame content	✔	✔	✔	✔	✔	✔	✔	
Ethertype mutation	✔	✔	✔	✔	✔	✔	✔	
Counter length (in bytes)	5	5	5	5	5	5	5	
Frame overhead unauthenticated encryption	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	0 (CFB)/ 8 (CTR)	8 (CTR)	8 (CTR)	
Frame overhead authenticated encryption (AE)	24	24	24	24	24	24*	24*	*GCM (Roadmap Q4 2017)
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔	
Tunnel (Ethernet over Ethernet)	*	*	*	*	*	* Roadmap Q4 2017	* Roadmap Q4 2017	
Max. number of peers	2	2	2	2				
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited				
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited				
Integrity protection (algorithm)	GCM	GCM	GCM	GCM				
Authentication length (bytes)	16	16	16	16				
Replay protection	✔	✔	✔	✔				
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames				
Counter length (in bytes)	5	5	5	5				
Frame overhead unauthenticated encryption	8 (CTR)	8 (CTR)	8 (CTR)	8 (CTR)				
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)	24 + tunnel (min. 18 bytes)				
Ethernet multi-hop support	✔	✔	✔	✔				

Senetas

Ethernet over IP (EoIP)							
Tunnel (Ethernet over IP)	*	*	*	*		* Roadmap Q4 2017	* Roadmap Q4 2017
Supported transmission protocols (UDP/TCP)	UDP/TCP	UDP/TCP	UDP/TCP	UDP/TCP			
Max. number of peers	2	2	2	2			
Max. number of MAC Addresses	unlimited	unlimited	unlimited	unlimited			
Max. number of VLAN IDs	unlimited	unlimited	unlimited	unlimited			
Integrity protection (algorithm)	GCM	GCM	GCM	GCM			
Authentication length (bytes)	16	16	16	16			
Replay protection	✔	✔	✔	✔			
Variable replay window (size)	256 frames	256 frames	256 frames	256 frames			
Counter length (in bytes)	5	5	5	5			
Frame overhead unauthenticated encryption	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)	8 (CTR) + tunnel (min. 38 bytes)			
Frame overhead authenticated encryption (AE)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)	24 + tunnel (min. 38 bytes)			
Ethernet multi-hop support	✔	✔	✔	✔			
Native IP Encryption							
Supported IP versions							
IPv4							
IPv6							
Supported transmission protocols							
TCP							
UDP							
Transport/Tunnel 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)							
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							
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔		Roadmap Q4 2017	Roadmap Q4 2017

Senetas

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	✔	✔	✔	✔	✔/QRNG	✔QRNG	✔/QRNG
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)							
RSA							
Key length	2048	2048	2048	2048	2048	2048	2048
Elliptic Curve Cryptography (ECC)							
Key length	512	512	512	512	512	512	512
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
Device Authentication							
Symmetric Signature: Pre-shared Key (PSK)							
Maximum number of PSKs per encryptor							
Key length							
Asymmetric Signature: Certificate	x.509	x.509	x.509	x.509	x.509	x.509	x.509
Maximum number of certificates per encryptor	64	64	64	64	64	64	64
Key length	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)	512 (ECC)/2048 (RSA)
Ad-hoc authentication of peers (manual)							
Signature key protocol	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA	ECDSA/RSA
Key Agreement and Key Exchange							
Master Key (KEK) Agreement	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA	ECDH/RSA
Master Key (KEK) Exchange Protocol	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas	Senetas
Automatic Change of Master Key	✔	✔	✔	✔	✔	✔	✔
Minimum suggested Time Interval for Master Key Change (min)	1440	1440	1440	1440	1440	1440	1440
Separate Master Key (KEK) per site	✔	✔	✔	✔	✔	✔	✔
Separate Master Key (KEK) per group	✔	✔	✔	✔	✔	✔	✔
Session Key (DEK) Exchange Agreement	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications	ATM Forum Security Specifications
Session Key (DEK) Exchange Protocol	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A	NIST SP800-56A
Automatic Change of Session Keys	✔	✔	✔	✔	✔	✔	✔
Minimum Time Interval for Session Key Change (min)	1	1	1	1	1	1	1

Senetas

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)	✔	✔	✔	✔	✔	✔	✔

Senetas

Network Support								
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔	
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔	
Ethernet Flow Control via PAUSE								
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)	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	RO/RW	
TLS								
Proprietary								
Remote Monitoring (SNMP)	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	v1/v2c/v3	
Logs								
Event Log (local)	✔	✔	✔	✔	✔	✔	✔	
Audit Log (local)	✔	✔	✔	✔	✔	✔	✔	
Syslog Support (Server)	✔	✔	✔	✔	✔	✔	✔	
Unit								
Height in 19" Rack	Desktop	Desktop	1U	1U	4U	1U	1U	
Number of external encrypted Ethernet ports	1	1	1	1	1-10	1	1	
Physical Device Access	back	back	front	front	front	front	front	
Redundant Power Supply			✔	✔	✔	✔	✔	
Redundant, hot-swappable power supply			✔	✔	✔	✔	✔	
High Availability functionality (two-node cluster)	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	Roadmap 2017	
MTBF	> 200.000h	> 200.000h	> 200.000h	> 200.000h	> 100.000h	> 200.000h	> 200.000h	
Tamper Security	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	
Security Approvals	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+, UC APL, NATO	FIPS140-2 L3, CC EAL2+	FIPS140-2 L3/CC EAL2+ in progress	*	CC EAL2+, FIPS 140-2 L3, UC APL/CPA in progress/planned
Safety Approvals	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000 ROHS	EN55022 class B, EN61000, ROHS	EN55022 class B, EN61000, ROHS	
Boot Time								
Cold boot until operational (P2P)	65s	65s	65s	65s	65s	65s	65s	
Warm boot until operational (P2P)	80s	80s	80s	80s	80s	80s	80s	

* For CN 9100 CC EAL2+ in progress, for CN 9120, FIPS 140-2 L3 and CC EAL2+ planned. For both: UC APL and NATO planned

Senetas

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
	Number of roles	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)	3 (SMC)/4 (CM7)
	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 €)		on request	on request	on request	on request	on request	on request	on request
Per external Key Server (in €); optional, no requirement, starting price		on request	on request	on request	on request	on request	on request	on request
Required Management Software		CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included	CM7 included
Optional SMC Sofware	1-4 encryptors	free	free	free	free	free	free	free
	5-10 encryptors	on request	on request	on request	on request	on request	on request	on request
	11-20 encryptors	on request	on request	on request	on request	on request	on request	on request
	unlimited	on request	on request	on request	on request	on request	on request	on request
Warranty Period (months)		12	12	12	12	12	12	12
Warranty Coverage	Parts & Work	✔	✔	✔	✔	✔	✔	✔
	Basic Support (9 to 5, e-mail, phone)	✔	✔	✔	✔	✔	✔	✔
	Software updates and upgrades	✔	✔	✔	✔	✔	✔	✔
Warranty Extension (per year)		15%	15%	15%	15%	15%	15%	15%%

* Additionally available: Premium support (24x7 support, Advance RMA) with Plus Maintenance

Thales E-Security

	Datacryptor 5100	Datacryptor 5100	Datacryptor 5200	Datacryptor 5300	Datacryptor 5400	40G	100G
Line Interface/Supported Line Rates							
						Roadmap Q2 2017	Roadmap Q4 2017
10 Mbs	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP			
100 Mps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+		
1 Gbps	✔/RJ45	✔/RJ45	✔/RJ45	✔/SFP	✔/SFP+	✔/QSFP	
10 Gbps				✔/SFP	✔/SFP+	✔/QSFP	✔/QSFP28
25Gps						✔/QSFP	✔/QSFP28
40 Gbps						✔/QSFP	✔/QSFP28
100 Gbps							✔/QSFP28
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	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔
Supported Networks (Transport of Encrypted Frame)							
Ethernet (native)	✔	✔	✔	✔	✔	✔	✔
MPLS (EoMPLS)	✔	✔	✔	✔	✔	✔	✔
IPv4/IPv6	✔	✔	✔	✔	✔	✔	✔
TCP	✔	✔	✔	✔	✔	✔	✔
UDP	✔	✔	✔	✔	✔	✔	✔
Supported Usage Scenarios							
Single tenant	✔	✔	✔	✔	✔	✔	✔
Multi-tenant	✔	✔	✔	✔	✔	✔	✔
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
Key Management	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia	atmedia

Thales E-Security

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	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs
store & forward	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs
Latency MP Mode cut-through	<42µs	<8µs	<42µs	<8µs	<4µs	<4µs	<2µs
store & forward	<48µs	<9µs	<48µs	<9µs	<4µs	<4µs	<2µs
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
Replay protection	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8
Frame overhead (unauthenticated encryption)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead (authenticated encryption)	18/26	18/26	18/26	18/26	18/26	18/26	18/26
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	256	unlimited	256	unlimited	256	unlimited	256
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
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	✔	✔	✔	✔	✔	✔	✔
Ethertype mutation (unauthenticated encryption only)	✔	✔	✔	✔	✔	✔	✔
Counter length (in bytes)	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	18/26	18/26	18/26	18/26	18/26	18/26	18/26
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
Replay protection	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8
Frame overhead unauthenticated encryption	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Frame overhead authenticated encryption (AE)	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*	30/38*
Ethernet multi-hop support	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

Thales E-Security

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
Replay protection	✔	✔	✔	✔	✔	✔	✔
Variable replay window (size)	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s	✔ 0-30s
Counter length (in bytes)	8	8	8	8	8	8	8
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 Tunnel Mode							
Maximum number of peers	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited
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)	8	8	8	8	8	8	8
Packet overhead authenticated encryption (AE)	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66	IPv4: 38/46, IPv6: 58/66
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	✔	✔	✔	✔	✔	✔	✔
Traffic Masking							
Traffic Flow Security	✔	✔	✔	✔	✔	✔	✔

*IMIX=100%

**TFS mode only secure based on ASIC or FPGA

Thales E-Security

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	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP	TE/TP
Asymmetric Key Algorithms (Public Key Cryptography)							
RSA							
Key length	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Elliptic Curve Cryptography (ECC)							
Key length	512/521	512/521	512/521	512/521	512/521	512/521	512/521
Supported Curves:							
NIST	✔	✔	✔	✔	✔	✔	✔
Brainpool	✔	✔	✔	✔	✔	✔	✔
Custom Curves	✔	✔	✔	✔	✔	✔	✔
Hash Algorithms							
SHA-2 Key length	512	512	512	512	512	512	512
CBC-MAC-GCM Key length	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
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
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

***ECDSA optional for use with optional certificates

*****NIST, Brainpool or custom curves with 256 to 521 bit length

Thales E-Security

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)	✔	✔	✔	✔	✔	✔	✔

Thales E-Security

Network Support							
Bump in the Wire deployment	✔	✔	✔	✔	✔	✔	✔
Jumbo Frame Support	✔	✔	✔	✔	✔	✔	✔
Ethernet Flow Control via PAUSE	✔	✔	✔	✔	✔	✔	✔
Ethernet Fragmentation/Defragmentation	✔	✔	✔	✔	✔	✔	✔
Point-to-Point	✔	✔	✔	✔	✔	✔	✔
Point-to-Multipoint	✔	✔	✔	✔	✔	✔	✔
Multipoint	✔	✔	✔	✔	✔	✔	✔
Dead Peer Detection	✔	✔	✔	✔	✔	✔	✔
Optical Loss Pass-Through	N/A	N/A	N/A	✔	✔	✔	✔
Link Loss Carry Forward	✔	✔	✔	✔	✔	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	1	1-4	1-4
Physical Device Access	back	back	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 *	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 in progress	FIPS 140-2 L3 iplanned	FIPS 140-2 L3 planned
Safety Approvals	EN55032 Class B, FCC Part 15 Class B, ROHS						
Boot Time							
Cold boot until operational	25s	25s	25s	25s	25s	25s	25s
Warm boot until operational	27s	27s	27s	27s	27s	27s	27s

* Products using the platform have BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL) approvals

Thales E-Seccurity

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
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)	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
Warranty Extension (per year)	on request	on request	on request	on request	on request	on request	on request

Viasat

	SEC-1140V	SEC-1170	
Line Interface/Supported Line Rates			
10 Mbs	✔		
100 Mps	✔		
1 Gbps	✔		
10 Gbps		✔/SFP+	
25Gps		✔/SFP28	
40 Gbps		✔/QSFP	
100 Gbps		✔/QSFP28	
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	✔	✔	
IPv4/IPv6			
Supported Networks (Transport of Encrypted Frame)			
Ethernet (native)	✔	✔	
MPLS (EoMPLS)	✔	✔	
IPv4/IPv6			
TCP	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	EoIP only
UDP	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	EoIP only
Supported Usage Scenarios			
Single tenant	✔	✔	
Multi-tenant			
Self-managed	✔	✔	
Managed encryption service	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	
Managed security service	Roadmap Q4 CY 2017	Roadmap Q4 CY 2017	
Platform			
Platform used			
Mainboard/Firmware	ViaSat/ViaSat	ViaSat/ViaSat	
Key Management	MKA/EAPOL-TLS	MKA/EAPOL-TLS	

		Viasat	
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	N/A	<3μs
Latency MP Mode	cut-through		
	store & forward	N/A	<3μs
Encryption Modes			
Native Ethernet Encryption			
Frame Encryption (Bulk - P2P only)			
	Integrity protection (algorithm)		
	Authentication length (bytes)		
	Replay protection		
	Variable replay window (size)		
	Counter length (in bytes)		
	Frame overhead (unauthenticated encryption)		
	Frame overhead (authenticated encryption)		
	Ethernet multi-hop support		
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
	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	✔	✔
	Ethertype mutation (unauthenticated encryption only)		
	Counter length (in bytes)	8	8
	Frame overhead unauthenticated encryption		
	Frame overhead authenticated encryption (AE)	32	32
	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)		
	Replay protection		
	Variable replay window (size)		
	Counter length (in bytes)		
	Frame overhead unauthenticated encryption		
	Frame overhead authenticated encryption (AE)		
	Ethernet multi-hop support		

Feature	Viasat	
Ethernet over IP (EoIP)		
Tunnel (Ethernet over IP)	Roadmap Q4 CY2017	Roadmap Q4 CY2017
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)		
Replay protection		
Variable replay window (size)		
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/Tunnel 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)		
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	Roadmap Q4 CY2017	Roadmap Q4 CY2017
IP		
Based on presence of MPLS tag		
MPLS	✔	✔
EoIP	Roadmap Q4 CY2017	Roadmap Q4 CY2017
IP		
Based on VLAN ID and presence of MPLS tag		
MPLS	✔	✔
EoIP	Roadmap Q4 CY2017	Roadmap Q4 CY2017
IP		
Traffic Masking		
Traffic Flow Security	Roadmap Q4 CY2017	Roadmap Q4 CY2017

	Viasat		
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	Roadmap Q4 CY2017	Roadmap Q4 CY2017	
External Key Server	Roadmap Q4 CY2017	Roadmap Q4 CY2017	
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	✔ (dependent on CPU)	✔	VNF requires Intel RDRAND (Hardware TRNG) built into all Xeons
Tamper Security Key Storage (tamper-evident or tamper-proof)	N/A	TE/TP	
Asymmetric Key Algorithms (Public Key Cryptography)			
RSA			
Key length			
Elliptic Curve Cryptography (ECC)			
Key length	384	384	
Supported Curves:			
NIST	✔	✔	
Brainpool			
Custom Curves			
Hash Algorithms			
SHA-2 Key length	512	512	
Device Authentication			
Symmetric Signature: Pre-shared Key (PSK)	✔	✔	Connectivity Association Key (CA), also used for Key derivation to get SAKs and KEKs
Maximum number of PSKs per encryptor	512	512	
Key length	256	256	256-bit CAKs and a 128-bit CAK-Name (CKN) which is cryptographically derived from the CAK.
Asymmetric Signature: Certificate	x.509	x.509	Certificates used for asymmetric exchange and key derivation exchange
Maximum number of certificates per encryptor	1	1	Only 1 certificate currently supported - due to market re-analyzing when multi-tenant support will be added.
Key lenght			
Ad-hoc authentication of peers (manual)	✔	✔	
Signature key protocol	ECDSA w/SHA384	ECDSA w/SHA384	
Key Agreement and Key Exchange			
Master Key (KEK) Agreement	TLS 1.2	TLS 1.2	
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)	5	5	

Certificates have to be provisioned onto units via management port. at our factory with a unique cert per unit.
Currently units are shipped with a ViaSat default Certificate per unit, and are then pre-provisioned

Key System		Viasat	
Point-to-Point Key System			
Supported key system			
	Pairwise	✔	✔
	Group	Unidirectional Group	Unidirectional 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	Roadmap Q2 2017	Roadmap Q2 2017
	IP Address		
	IP Muticast Group		
Group Key Distribution			
	Unicast (unique KEK per group member)	✔	✔
	Broadcast (same KEK for all group members)	✔	✔

	Viasat		
Network Support			
Bump in the Wire deployment	✔	✔	
Jumbo Frame Support	✔	✔	
Ethernet Flow Control via PAUSE	✔	✔	
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	Roadmap Q3 CY2017	Roadmap Q3 CY2017	
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	N/A	1	
Number of external encrypted Ethernet ports	unrestricted	up to 4	
Physical Device Access	N/A	front	
Redundant Power Supply			
Redundant, hot-swappable power supply		✔	
High Availability functionality (two-node cluster)	1-1	1-1	
MTBF			
Tamper Security	N/A	TE/TP	
Security Approvals		FIPS-140-2 Level 3 CY2017, NIAP/CC EAL-4	All planned; FIPS is in process.
Safety Approvals		EN55022 class B - FCC Part 15 Class B	
Boot Time			
Cold boot until operational (P2P)	560s	120s	
Warm boot until operational (P2P)	560s	120s	

Viasat

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	Roadmap Q2 CY2017	Roadmap Q2 CY2017
	Certificate Management	Roadmap Q2 CY2017	Roadmap Q2 CY2017
Key Management			
	Group creation	✔	✔
	Group isolation	✔	✔
	Key assignment	✔	✔
	Fail-over configuration	✔	✔
Price			
List Price Encryption Unit (in €)	1G VNF, or 10G SEC-1170	on request	on request
List Price Encryption Unit (in €)	4x10G, 4x25G		on request
List Price Encryption Unit (in €)	100G		on request
Per external Key Server (in €)			
Required Management Software			
	2-10 encryptors		
	11-25 encryptors		
	26-50 encryptors		
	51+ encryptors		
Warranty Period (months)		12	12
Warranty Coverage	Parts & Work		
	Basic Support (9 to 5, e-mail, phone)		
	Software updates and upgrades		
Warranty Extension (per year)		✔	✔