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

© 2007-2017 Christoph Jaggi

All rights reserved.

www.uebermeister.com cjaggi@uebermeister.com

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION

| 1. ENCRYPTION LAYER AND SECURITY | 1 |
|----------------------------------|---|
| 2. DIFFERENT APPROACHES | 2 |
| 2.1 Hop-by-Hop vs. End-to-End | 2 |
| 2.2. Dedicated vs. integrated | 3 |
| 3. Criteria and coverage | |
| 3.1. Criteria | 5 |
| 3.2. Coverage | 6 |
| 3.3. Objective | |
| J.J. Objective | 0 |

CHAPTER 2: MARKET OVERVIEW

| 1. VENDORS AND PRODUCTS | |
|---|---|
| | |
| 2. NETWORK STANDARDS AND PLATFORMS | |
| 2.1. ETHERNET INTERFACE AND DATA THROUGHPUT | 10 |
| 2.2. Supported Network Topologies | 11 |
| 2.2.1. Point-to-Point | |
| 2.2.2 Point-to-Multipoint | |
| 2.2.3. Multipoint-to-Multipoint | |
| 2.3. Supported Metro and Carrier Ethernet Topologies | |
| 2.4. NETWORKS SUPPORTED FOR ENCRYPTION | 13 |
| 2.5. NETWORKS SUPPORTED FOR THE TRANSPORT OF ENCRYPTED FRAMES | 14 |
| 2.6. Operating Scenario | 15 |
| 2.7. Platform Used | 16 |
| 2.8. Operating Modes | 16 |
| | |
| | |
| 3. DATA PLANE ENCRYPTION | |
| 3. DATA PLANE ENCRYPTION | |
| | 18 |
| 3.1. ENCRYPTION STANDARD | |
| 3.1. Encryption Standard3.2. Encryption Hardware | 18 18 19 |
| 3.1. ENCRYPTION STANDARD3.2. ENCRYPTION HARDWARE3.3. PROCESSING METHOD | |
| 3.1. ENCRYPTION STANDARD 3.2. ENCRYPTION HARDWARE 3.3. PROCESSING METHOD | |
| 3.1. ENCRYPTION STANDARD | $ \begin{array}{cccccccccccccccccccccccccccccccccccc$ |
| 3.1. ENCRYPTION STANDARD | $ \begin{array}{cccccccccccccccccccccccccccccccccccc$ |

2017 Market Overview Ethernet Encryptors for Metro und Carrier Ethernet (short version)

| 3.9. Traffic Flow Security | 26 |
|---|------|
| 4. Control Plane Security | . 27 |
| 5. Auto-Discovery and Key Server | . 28 |
| 5.1. Auto-Discovery | 28 |
| 5.2. Key Server | 28 |
| 5.3. INTEGRATED KEY SERVER | 28 |
| 5.4. Support for External Key Server | |
| 5.5. External Key Server | |
| 5.6. Support for Multiple, Distributed Key Servers | 29 |
| 5.7. SUPPORT FOR FAIL-OVER TO BACKUP KEY SERVER | |
| 6. Key Management | . 30 |
| 6.1. Basic Equipment | 30 |
| 6.1.1. Hardware Random Number Generator | |
| 6.1.2. Secure Key Storage | |
| 6.1.3. Autonomous Operation | |
| 6.2. Connectivity Association | 31 |
| 6.3. AUTHENTICATION/INITIAL SECRET AND SIGNATURE PROTOCOL | 32 |
| 6.4. Key Exchange | 33 |
| 6.4.1. Symmetrical Key Exchange | 33 |
| 6.4.2. Asymmetrical Key Exchange | |
| 6.4.3.Exchange Frequency | |
| 6.5. Кеу System | |
| 6.4.1.Pairwise Keys | |
| 6.4.2. Group Keys | 38 |
| 7.Network Support | |
| 7.1. BUMP-IN-THE-WIRE-DEPLOYMENT | - |
| 7.2. Jumbo Frames | |
| 7.3. Ethernet Flow Control | |
| 7.4. Fragmentation | |
| 7.5. Dead Peer Detection | |
| 7.6. Optical Loss Pass-Through | |
| 8.7. Link Loss Carry Forward | 44 |
| 8. System Management | . 45 |
| 8.1 Out-of-Band Management | |
| 8.2 In-Band Management | 45 |
| 8.3 Slots and Ports | 45 |
| 8.4 SNMP | 45 |
| 8.5 Logs | 46 |
| 9. UNIT | . 47 |

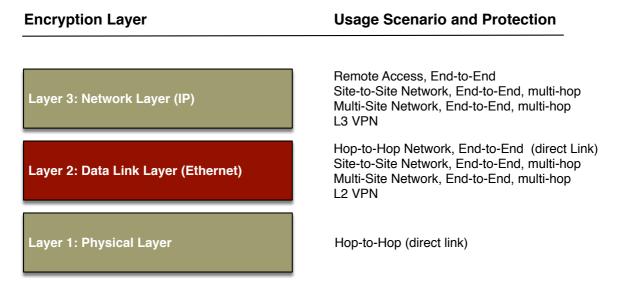
2017 Market Overview Ethernet Encryptors for Metro und Carrier Ethernet (short version)

| 9.1 Rack Unit | |
|---|----|
| 9.2 Device Access | 47 |
| 9.3 REDUNDANT POWER SUPPLIES | |
| 9.4 Mean Time between Failures | 47 |
| 9.5 High Availability | |
| 9.6 Device Protection | |
| 9.7 Security Approvals | |
| 9.8 Security Relevant Approvals | 49 |
| | |
| 10. MANAGEMENT-SOFTWARE | 50 |
| 10.1 MANAGEMENT ACCESS | 50 |
| 10.2 Device Management | 50 |
| 10.3 Certificate Authority und Management | 50 |
| 10.4 Key Management | 51 |
| | |
| 12. PRICE AND WARRANTY | 52 |
| 12.1 PRICE | |
| 12.2 Operating Cost | |
| 12.3 WARRANTY AND WARRANTY COVERAGE | |
| | |

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.



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

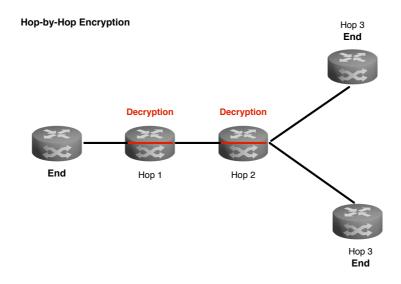
For network encryption there are different approaches and practices. They have a direct impact on the application scenarios supported and the security level provided by a solution.

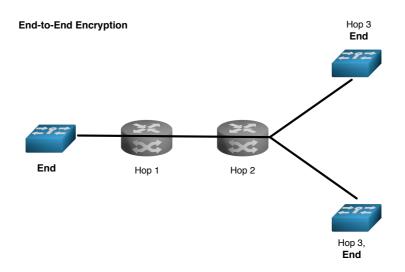
There are different possibilities to encrypt Ethernet networks. It can be done at layer 1, layer 2 and layer 3. It is most efficient at layer 1 and layer 2, and most flexible at layer 2 and layer 3. The optimal combination of efficiency and flexibility is provided by Ethernet encryption at layer 2. Even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

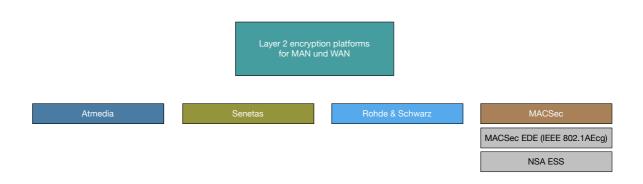
Thales

(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

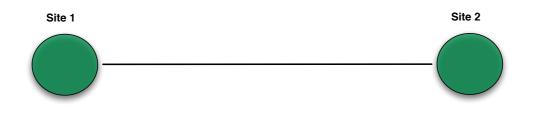
security and performance depends on the operating environment. The characteristics of the hardware available to the virtual appliance are essential. Without dedicated and optimized hardware not all crucial functions have direct hardware support anymore, despite still being available. This leads to a 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.

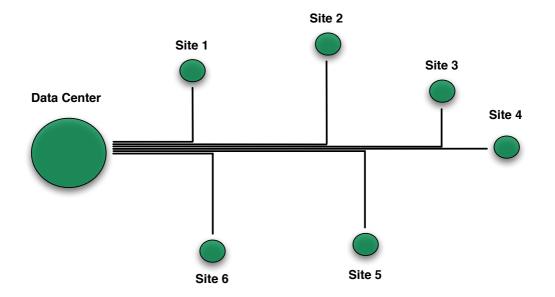
2.2.1. Point-to-Point

A point-to-point connection connects two sites.



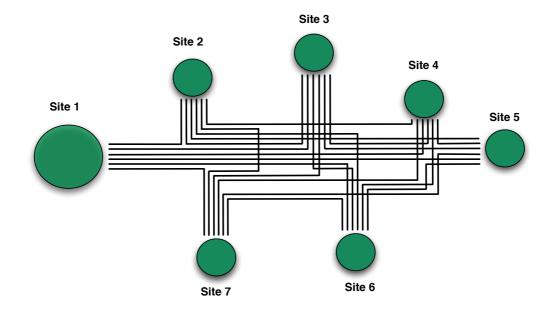
2.2.2. Point-to-Multipoint

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



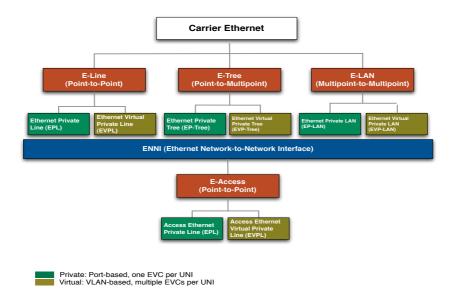
2.2.3. Multipoint-to-Multipoint

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.

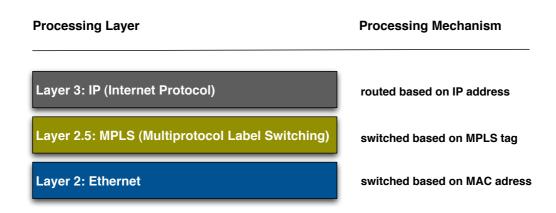


2.4. Networks Supported for Encryption

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.

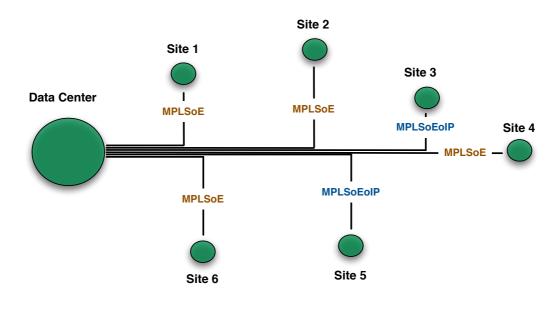
It is not common practice yet to secure mixed environments with a single encryptor yet. Often a different encryptor is used for layer 2 and layer 3.



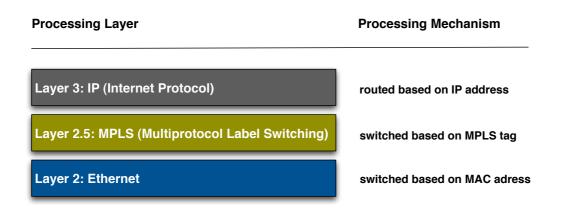
2.5. Networks Supported for the Transport of Encrypted Frames

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.

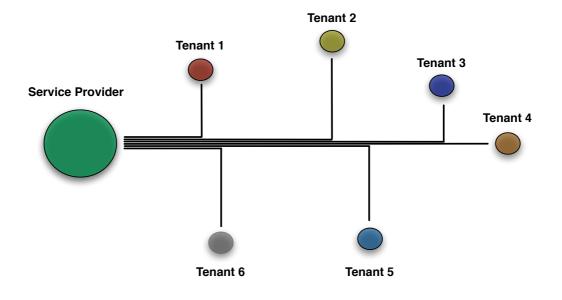


The demands in terms of encryptor functionality are substantially increased, as next to the frame transport over IP also key exchange over IP has to be supported.



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-topoint 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-topoint 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

| DA | SA | ET | VID | ET | IV | ET | Payload | ICV | CRC |
|----|----|------------------------|---------------|-----|----------------------|----|----------------------------------|---|-----------------------|
| | | AC He (18 by | eader tes) | | SecTag (10 bytes) | | Data (16 - 1500 bytes) | Integrity Check Value (8 - 16 bytes) | Checksum (4 bytes) |
| - | | | | aut | henticated | | - encrypted | | |

Frame mode with authenticated encryption

Advantages:

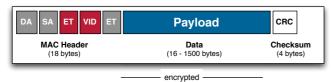
- All frames are completely encrypted
- Tapping the line will reveal nothing concerning network and data
- Authenticated encryption generates little overhead (24-32 bytes) compared to the security gained
- If unauthenticated, there is no encryption overhead on frame level

Disadvantages:

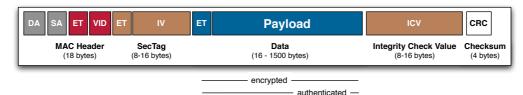
- Needs dedicated line
- Cannot be switched
- Has higher operating cost
- Incompatible with Managed Ethernet Services

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

| DA SA ET VID | ET | IV | DA | SA | ET V | ID E | Payload | | ICV | CRC |
|--------------------------|----|----|---|----|------|------|-----------|-----------------------------------|-----------------------|-----|
| MAC Header (18 bytes) | | | MAC HeaderData(18 bytes)(16 - 1500 bytes) | | | | | Integrity Check (4 - 18 bytes) | Checksum (4 bytes) | |
| authenticated | _ | | _ | | | | encrypted | _ | | |

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.

| DA SA ET VID ET | IPv4 Header | TCP Header | DA SA ET VID E | r iv | ET | Payload | ICV | CRC | CRC |
|--------------------------------------|-------------------------------|-------------------------------|--------------------------|----------------------|----|----------------------------------|---|-----------------------|-----------|
| Local Transport Header (18 bytes) | Delivery Header (20 bytes) | Delivery Header (20 bytes) | MAC Header (18 bytes) | SecTag (10 bytes) | | Data (16 - 1500 bytes) | Integrity Check Value (8 - 16 bytes) | Checksum (4 bytes) | (4 bytes) |

Ethernet over IP (EoIP) over TCP with authenticated encryption

| DA SA ET VID ET | IPv4 Header | UDP Header | DA SA ET | VID ET | IV | ET | Payload | ICV | CRC | CRC |
|--------------------------------------|-------------------------------|------------------------------|-----------------|--------|----------------------|----|----------------------------------|---|-----------------------|-----------------------|
| Local Transport Header (18 bytes) | Delivery Header (20 bytes) | Delivery Header (8 bytes) | MAC H (18 by | | SecTag (10 bytes) | | Data (16 - 1500 bytes) | Integrity Check Value (8 - 16 bytes) | Checksum (4 bytes) | Checksum (4 bytes) |

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.

| IP Header | SecTag | Payload | ICV | | | | | | | |
|----------------------------|------------------|----------------------------------|---------------------------------------|--|--|--|--|--|--|--|
| IP Header (20/40 bytes) | IV (10 bytes) | Data (16 - 1500 bytes) | Integrity Check Value (8-16 bytes) | | | | | | | |
| | | encrypted | _ | | | | | | | |
| authenticated | | | | | | | | | | |

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.

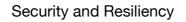
3.9. Traffic Flow Security

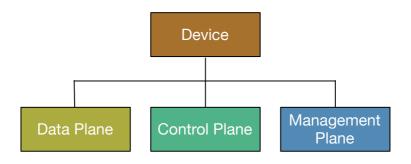
Traffic flow security obfuscates the actual data traffic by changing frame sizes and frame sequences during transport. Traditional methods were limited to using uniform frame sizes and to dedicated point-to-point scenarios. Newer methods work with variable frame sizes and support all usage scenarios. 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

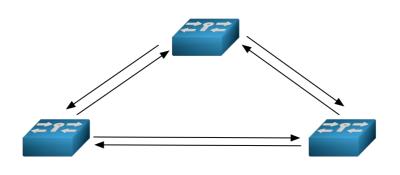
6.1.3. Autonomous Operation

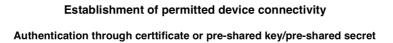
Autonomous operation requires that the encryptor accomplish its job independently of external resources. Each external resource constitutes a risk and a dependency. Dedicated key servers, certificate authorities and dedicated security management are not considered to be external resources. Such devices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

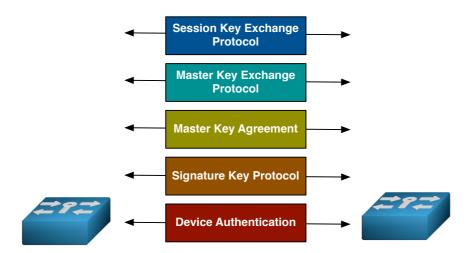
Connectivity Association





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.

| Кеу Туре | 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 |

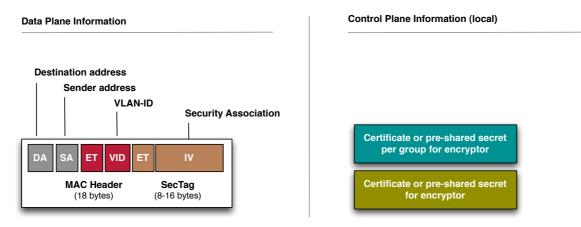
6.5. Key System

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.

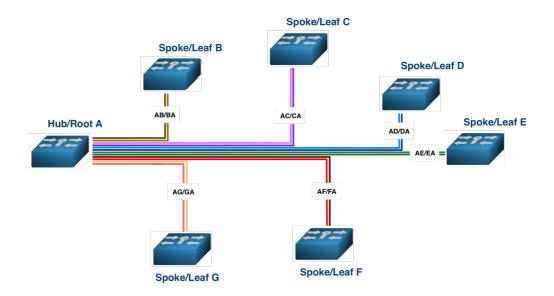
Further it is possible to use a combination of a pairwise and a group key system. From an organizational point of view a VLAN can constitute a group, in which pairwise keys are used for unicast traffic and a group key is used for multicast and broadcast traffic. For each VLAN separate pairwise keys and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

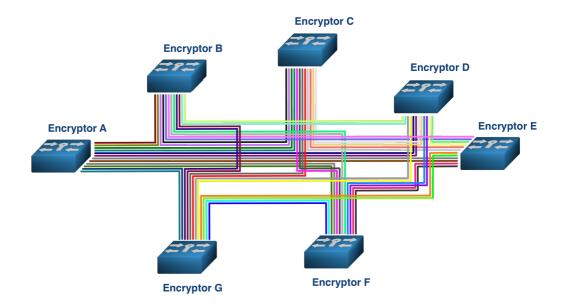


Pairwise keys systems are designed for point-to-point connections and therefore also treat point-to-multipoint and multipoint networks as an accumulation of point-to-point connections.



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.

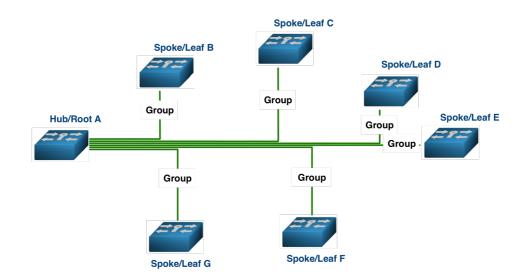
6.5.2. Group Keys

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,

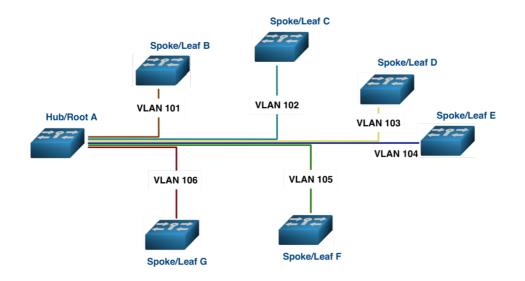
This works for all three basic topologies, starting with point-to-point:



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

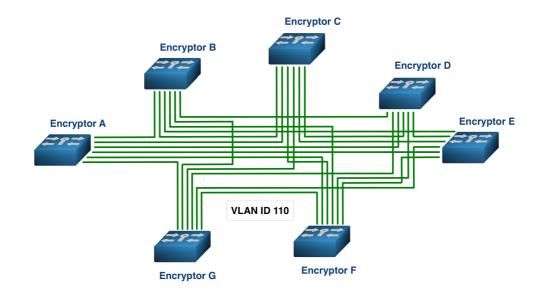


Or each connection between the hub and a spoke is treated as a single group.

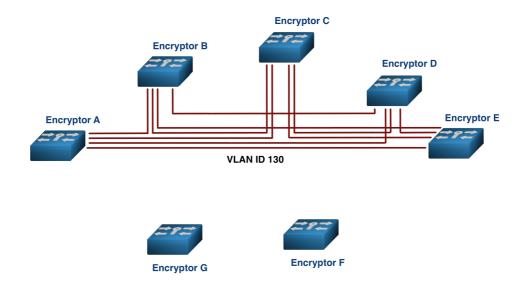


It is also possible to use a mix between the two approaches.

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.

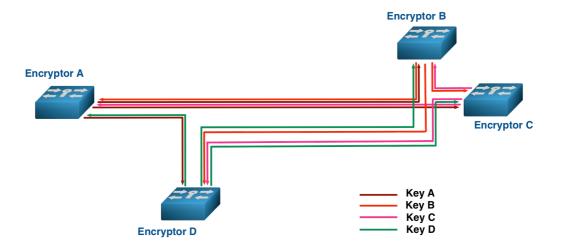


Multipoint connections often are groups that share a common broadcast domain. Within a group all data traffic is encrypted with the same session key. There is no differentiation between unicast, multicast and broadcast frames.

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 encryptor, every group member distributes the key he is using for encrypting his outgoing data traffic to all other group members. In such a scenario, each encryptor is also the key server for his keys.



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

7. Network Support

7.1. Bump-in-the-Wire Deployment

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

7.2. Jumbo Frames

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

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

7.3. Ethernet Flow Control

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

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

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.

| up undrace/supported Lupe Reter visite <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> | | | | | | | | |
|--|-----------------|--------|-------------------------|---|--------|--------|-----|--|
| Under CPP-Lubi Virue Virue Virue Virue Virue Virue </td <td>, ,</td> <td>, ,</td> <td>• •</td> <td>, ,</td> <td>• •</td> <td>、、</td> <td>、、</td> <td></td> | , , | , , | • • | , , | • • | 、、 | 、、 | |
| YING | ۲, | ۲, | ۲, | ۲, | ۲, | ٩, | ۲, | IPv4/IPv6 |
| Image: Section of the section of th | , , | , , | , , | , , | , , | , , | , , | Ethernet (native) MPI S (EAMPI S) |
| Vinio Vinio </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> | | | | | | | | |
| · Ling · Ling <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>innorted Networks (Transnort of Encrypted Frame)</td> | | | | | | | | innorted Networks (Transnort of Encrypted Frame) |
| VN (EVP-TW) V. C. V. | ۲ | ٢ | ۲ | ۲ | ۲ | ٢ | ۲ | IP v4/v6 |
| AN (EXP-TAN) AN (E | ۰ , | ۰, ۲ | ۰ ، | ۲, | ۲, | ۲, | ۰ ، | MPLS |
| AL FASION C C C C C C C C C C C C C C C C C C C | ¢ | ¢ | ¢ | ¢ | ¢ | ¢ | ¢ | Ethernet |
| ALIENDE-TAN) LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE-TAN LIENDE LIEN | | | | | | | | upported Networks (Encryption) |
| Indicating in the contract of the c | • | • | • | • | • | • | • | בעופווופן עוועמן רוע מפ באוע (בעריבאוע) |
| Herr-Additional and | < · | < • | ς • | : • | | < • | | Ethernet Virtual Drivete I AN (EVPJ AN) |
| Line | | | | | | | | Ethernet Virtual Private Line (EVP-Line) |
| Internal of the second | | | | | | | | |
| V-MN X X X X <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> | | | | | | | | |
| Image: strategy of the strategy of | ۲ | ٢ | ۲ | ۲ | ۲ | ۲ | ۲ | Ethernet Private LAN (EP-LAN) |
| -Line | ۲ | ٢ | ٢ | ٢ | ۲ | ٢ | ۲ | Ethernet Private Tree (EP-Tree) |
| Image: Second | ۲ | ۲, | ۲ | ۲ | ۲ | ۲ | ۲ | |
| Image: Second | | | | | | | | Port-based |
| ales | | | | | | | | upported Metro Ethernet Topologies |
| ares | | | | | | | | |
| ates | ٢ | ٢ | ٢ | ٢ | ٢ | ٢ | ۲ | Multipoint (MP) |
| ates | ۲ | ۲ | ۲ | ۲ | ۲, | ۲ | ۲ | Point-to-Multipoint (P2MP) |
| ates | ٢ | ٢ | ۲ | ٢ | ۲ | ٢ | ۲ | Point-to-Point (P2P) |
| ates | | | | | | | | upported Network Topologies |
| Image: Constraint of the second of the se | | | | | | | | |
| VIRU45 VIRU45 VIRU45 VIRU45 VIRU45 VIRU45 VIRU45 VISEPP VIRU45 VIRU45 VISEPP VISEPP VISEP VISEPP VISEPP VISEPP | | | | | | | ۲ | Virtual Appliance |
| VIRLAS | | | | | | | | |
| VIRLAS VIRLAS VIRLAS VIRLAS VIRLAS VISEP VIRLAS VIRLAS VISEP VIRLAS VIRLAS VISEP | | | | | | | < < | 100 Ghne |
| v v/R445 v/R445 v/R445 v v/R45 v/R445 v/R445 v/R45 v/R45 v/R45 v/R45 v/R45 v/R45 v/R45 v/SFP v/SFP v/SFP v/SFP | € AQSEP | | | | | | . < | 25 ups |
| VIRUAS VIRUAS VIRUAS | ✔/USHP | ✓/SFP+ | ✓/SFP | | | | . < | 10 Gbps |
| ✓ ✓ | ✓/QSFP | ✓/SFP+ | ✓/SFP | ✔/RJ45 | ✔/RJ45 | ✔/RJ45 | ۲, | 1 Gbps |
| ✓ IRus ✓ IRus ✓ IRus ✓ IRus ✓ IRus | | ✓/SFP+ | ✓/SFP | <td>✔/RJ45</td> <td>✔/RJ45</td> <td>۲</td> <td>100 Mps</td> | ✔/RJ45 | ✔/RJ45 | ۲ | 100 Mps |
| | | | ✓/SFP | ✓/RJ45 | ✔/RJ45 | ✔/RJ45 | ۲ | 10 Mbs |
| | Roadmap Q2 2017 | п | | | | | | |
| | | | | | - | | | ne Interface/Supported Line Rates |

Platform

Platform used

Mainboard/Firmware Key Management

atmedia atmedia

atmedia/atmedia atmedia/atmedia atmedia/atmedia atmedia/atmedia atmedia/atmedia atmedia/atmedia atmedia/atmedia atmedia atmedi

atmedia atmedia Self-managed Managed encryption service Managed security service

, , ,

, , ,

, , ,

, , ,

, , ,

. . .

. . .

۰ ۲

ς ς

ς ς

ς ر

ς ς

۲ ۲

۲ ۲

۲ ۲

Single tenant Multi-tenant

| Tunnel (Ethernet) Max. number of VAN Des Max. number of VAN Des Reglay protection Reglay protection Reglay protection Variable reglay. (in bytes) Frame overhead authenticated encryption (AE) Ethernet multi-hop support | Transport (Payload only) Max. number of peers Max. number of MAC Addresses Max. number of VLAN IDs Integrity protection (algorithm) Autivanciation (angorithm) Autivanciation (angorithm) Autivanciation (angorithm) Autivanciation (angorithm) Autivanciation (angorithm) Variable encryption offset (fixed) Variable encryption offset (fixed) Counte length (in bytes) Frame overhead authenticated encryption only) Frame overhead authenticated encryption Ethermet multi-hop support | Encryption Modes Native Ethernet Encryption Fame Encryption (Buk - P2P only) Integrity protection (algorithm) Authentication length (bytes) Replay protection Catable republy (into bytes) Fame overhead (unauthenticated encryption) Frame overhead (unauthenticated encryption) Ethernet multi-hop support | Latency Latency P2P Mode cut-through store & forward Latency MP Mode cut-through store & forward | cut-through stroe&forward FPGA AFIC CPU | Data Plane Encryption Standard and Processing Encryption Standard Block Cipher Preferred Mode of Operation Alemative Mode of Operation Key Length (in bit) Processing Method | |
|--|--|--|--|---|--|---------|
| Scrw NVA 30/38 [°] 30/38 [°] 30/38 [°] | 1000 unlimited GCM 8/16 8/16 18/26 NU/8 | SCN 876 NIA 1826 | NA NA NA | ,, ,, | AES GCM 256 | |
| unlimited GCM 8/16 8/308 8/308 | unlinted 256 ۲.875 876 876 876 876 876 876 | ССМ С с с ССМ 1826 NA NA | <42/1s <48/1s <42/1s <48/1s | , , , | AES GCM 256 | |
| vunimitied GCM 8 ° 3088° 30688° | unimited unimited 8/16 8/16 8/16 18/26 18/26 | ССМ С. С. С | <ଷ୍ମ୍ୟାର <ସ୍ମ୍ୟାର <ସ୍ମ୍ୟାର | , , , | AES GCM 256 | |
| vulimited GCM 8 CCM 8 CC | uniimad 256 876 876 876 876 876 876 876 876 | GCM GCM 876 NIA 1826 | <42µs <48µs <42µs <48µs | , , , | AES GCM 256 | Atmedia |
| unimited GCM 8 6 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 | ۱۱۵۵۵ unlimited GCNU Brie Brie Brie Brie Brie Brie Brie Brie | NA NA NA | ත්ස ක්ෂ ක්ෂ ක්ෂ ක්ෂ | , , , | AES GCM 256 | edia |
| uniimted GCM 8/6 8/0-30s 9/0-30s 9/0-30s 9/0-30s 9/0-30s 9/0-30s 9/0-30s | 11000 1256 8/6 8/6 8/6 8/6 8/6 8/6 8/6 8/6 8/6 8/ | NNA NA | ્નમક <્નમક <્નમક <્નમક | , , , | AES GCM 256 | |
| vnimted GCM 8 € 5 5 8 0 8 8 0 8 9 0 8 0 8 9 0 0 | 1000 vnlimited vnlimited NN 8 NN 8 NN 8 NN 8 NN 8 NN 8 NN 8 NN | NA 8 8 00 10 10 10 10 10 10 10 10 10 10 10 10 | <4µs <4µs <4µs <4µs | 、、、 | AES GCM 256 | |
| vulimited unlimited 8 C 8 C 8 C 8 C 8 C 8 C 8 C 8 C 8 C 8 | unimited 256 8 CCM 8 CCC | NA 8 8 8 10 10 10 10 10 10 10 10 10 10 10 10 10 | -2418 -2418 -2418 | 、、、 | AES GCM 256 | |
| *IMIX=10 | | | | | | |

X=100%

| Traffic Flow Security | Based on VLAN ID and presence of MPLS tag MPLS EoIP IP | Besed on presence of MPLS tag EolP MPLS tag EolP MPLS tag EolP IP | Mixed Ethernet, MPLS, EoIP and IP Support | Based on MAC Address Based on VLAN ID Based on Ethertype Based on Fuence of WPLS Tag Based on IP Address Combination of multiple selection criteria | Tunnei (Ethernet over IP) Supported transmission protocols (UDPTCP) Max. number of MAC Addresses Max. number of MAC Matterication (algorithm) Counter length (in bytes) Frame overhead nathenicated encryption Frame overhead authenicated encryption Frame overhead authenicated and poly Nathenicated authenicated and poly Frame overhead authenicated and encryption Frame overhead authenicated encryption Frame overhead authenicated and encryption Frame overhead authenicated encryption Frame overhead auth | Ethernet over IP (EoIP) |
|-----------------------|---|---|---|--|---|-------------------------|
| N/A** | 、、、 | ,,, ,,, | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | <pre>Pative PUDP 2 (P2P), 10PUDP unlimited unlimited GCM 6 (</pre> | |
| ۲ | , , , | | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | 2 (P2P), 1000 (MP) unimited GCM 8/6 8/6 8/6 8/6 8/6 8/6 8/6 8/6 8/6 8/6 | |
| ۲ | | | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | 2 (P2P), 1000 (MP) unlimited GCM 8//6 8//6 8//6 8//6 8//6 8//6 8//6 8// | |
| ۲ | | | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | 2 (P2P), 1000 (MP) unlimited GCM 8/16 8/16 8/16 8/16 S4/62 S | |
| ۲ | | | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | 2 (P2P), 1000 (MP) uniimited GCM 8/16 8/16 8/16 8/16 Uniimited uniimited uniimited GCM 8/16 8/16 8/16 8/16 8/16 | |
| ٦ | | | | <i>、、、、、、、、</i> | 2 (22P), 1000 (MP) unlimited GCM 8/16 8/16 8/16 8/16 54/62 54/62 8/16 8/16 8/16 8/16 8/16 8/16 | |
| ۲ | | | | 、、、、、、、 | answ (PUDP unimined unimi | |
| ٢ | | | | ***** | unlimited unlimited GCM S4/62 Unlimited unlimi | |

MIX=100%

| Key Agreement and Key Exchange Master Key (KEK) Agreement Master Key (KEK) Exchange Protocol Automatic Change of Master Key Minimum suggested Time Interval for Master Key Change (min) Separate Master Key (KEK) per group Sestor Key (DEK) per group Sestor Key (DEK) Exchange Agreement Sestor Key (DEK) Exchange Protocol Automatic Change of Sestor Key Minimum Time Interval for Sestor Key Change (min) | Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encryptor Key length Maximum number of certificates per encryptor Maximum number of certificates per encryptor Key length Ad-hoc authentication of peets (manual) Signature key protocol | Hash Algorithms SHA-2 Key length CBC-MAC-GCM Key length Device Authentication | HSA Key length Elliptic Curve Cryptography (ECC) Key length Supported Curves: NIST Brainpool Custom Curves | Key Mathagement Key Generation and Storage Hardware Random Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) Asymmetric Key Algorithms (Public Key Cryptography) Box | Support for external Key Server Support for external Key Server External Key Server Support for multiple distributed Key Servers Support for fail-over to badd-up Key Server Autonomous operation | Auto-discovery Auto-discovery of network encryptors Auto-discovery of VLAVs Auto-discovery of VLAVs Disabiling of auto-discovery Disabiling of auto-discovery Key Server |
|--|--|--|---|--|--|--|
|--|--|--|---|--|--|--|

256

256

256

256

256

256

256

256

| 11 | | |
|----|-----------|---------|
| ٢ | ,, ,, | * * * * |
| ٦ | ,,,,, | ,,,, |
| ¢. | ,,,,, | ,,,, |
| ٦ | ,, ,, | * * * * |
| ۲ | ,, ,, | * * * * |
| ۲ | ** ** | * * * * |
| ۲ | · · · · · | |
| s. | | * * * * |

| ,,, | 512/521 | N/A | with SC/HSM with SC/HSM: TE/TP |
|-------|---------|-----|-----------------------------------|
| ,,, | 512/521 | N/A | телтр |
| | 512/521 | N/A | ТЕЛР |
| , , , | 512/521 | NVA | ТЕЛР |
| ,,, | 512/521 | N/A | TE/TP |
| ,,, | 512/521 | N/A | TE/TP |
| ,,, | 512/521 | N/A | TE/TP |
| * * * | 512/521 | N/A | TE/TP |

| | | | | | | (1) | |
|--|---|-----|--|----------------------------|-----|--|---|
| AES-MAC/ECDSA**** | ۲ | 512 | 64 (recommended:18) 64 (recommended:1) | optional | 256 | 512 (recommended:18) | ۲ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional | 256 | 512 (recommended:18) | ۲ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional optional optional | 256 | 512 (recommended:18) 512 (reco | ۲ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional | 256 | 512 (recommended:18) | ۲ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional | 256 | 512 (recommended:18) | ٢ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional | 256 | 512 (recommended:18) | ٢ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional | 256 | 512 (recommended:18) | ٢ |
| AES-MAC/ECDSA**** | ٢ | 512 | 64 (recommended:18) | optional | 256 | 512 (recommended:18) | ٢ |
| AES-MAC/ECDSA*** AES-MAC/ECDSA*** AES-MAC/ECDSA*** AES-MAC/ECDSA*** AES-MAC/ECDSA*** AES-MAC/ECDSA*** AES-MAC/ECDSA*** AES-MAC/ECDSA*** The priore and the p | | | | | | | |

| - | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
|---|---|---------|---------|---|---|----|---|---------|--|
| | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| • | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| - | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| • | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| - | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| • | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| | ۲ | atmedia | atmedia | ٢ | ۲ | 60 | ۲ | atmedia | ECKAS-DH***** |
| | | | | | | | | | *****NIST, Brainpool or custom curves with 256 to 521 bit length |

Atmedia

| uroup Key Justrioution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAN ID Frames with MPLS tag IP Address IP Muticast Group | Group Membership Definition Multicast group membership Individual membership Network membership VLAN membership Trunked YLAN membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multicast group Individual key per broadcast group (VLAN ID) | Key assignment based on: MAC address (pairwise and mixed) Multicast groups (mixed) VLAN ID (group) Port Group (group) IP Address IP Multicast Group | Multipoint Key System Supported key systems: Painvise Group Mixed (painvise unicast, group multicast) | Key assignment based on: MAC Address VLAN ID Port Group IP Address | Point-to-Multipoint Key System Supported key systems: Patrvise Group | Key assignment based on: MCA doress VLAN ID Port Group IP Address | Key System Point-to-Point Key System Supported key system Pairvise Group |
|---|---|--|--|--|--|---|---|---|--|--|
| , , | ,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ٢ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Bidirectional Group | 、、、、、 | Sidirectional Group | ,,,,, | Sidirectional Group |
| | * * * * * | * * * * * * | ۲ | ~ ~ | * * * * * * * * | Bidirectional Group | * * * * * | Sidirectional Group | * * * * * | Sidirectional Group |
| र र | ,,,,, | * * * * * * | ۲ | , , | * * * * * * * * | Ridirectional Group | 、、、、、 | Ridirectional Group | ,,,,, | Ridirectional Group |
| , , | ,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ۶ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | S Bidirectional Group | ,,,,, | K Bidirectional Group | ,,,,, | Autor Bidirectional Group |
| , , | ,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ۶. | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Sidirectional Group | ,,,,, | K Bidirectional Group | ,,,,, | Autimedia oup Bidrectional Group |
| , , | ,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ۶ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Sidirectional Group | ,,,,, | K Bidirectional Group | ,,,,, | Pidirectional Group |
| , , | ,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ۶. | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Sidirectional Group | ,,,,, | K Bidirectional Group | ,,,,, | € Bidirectional Group |
| | * * * * * * | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ~ | | ***** | Sidirectional Group | ,,,,, | Sidirectional Group | ,,,,, | Bidirectional Group |

| Network Support Bump on the Wire deported Line of Frame Support Dead Peer Detection Optical Loss Paes-Trongh Unit I use Carry Forward System Configuration and Management Access IP40 IP40 System Configuration and Management Re 220/24 Unit I use Carry Forward System Configuration and Management USB Pert Shadt Log (local) Atadit Log (local) Saled Support (Server) Saled Support (Server) Prometary Perturbation and encrypted Enternet ports Physical Device Access Perturbation Physical Device Access Physical Device Access Pacturbation Physical Device Access Physical Device Access Ph |
|---|
|---|

| N/A N/A | N/A | dependent on server dependent on server 1:1 N/A N/A | N/A unrestricted N/A | | v2c/v3 | read-only | , , , , , , | | N/A S | * * * * | ररर | |
|------------|---|---|----------------------------|-------|--------|-----------|-------------|------------|------------|---------|-------|--|
| 25s 27s | | 1:1 > 50.000h TE/TP | 1U 1 back | | v2c/v3 | read-only | * * * * | • • | ۲ م | | , , , | |
| 25s 27s | BSI VS-NfD, NATO res | 1:1 > 50.000h TE/TP | back | | v2c/v3 | read-only | * * * * | , , | ۲ × ۲ | ,,,, | ,,, | |
| 25s 27s | tricted, EU Restrint (includ | 1:1 > 50.000h TE/TP | 1U front | | v2c/v3 | read-only | ,,,, | , , | ۲ N ۲ | ,,,, | ,,, | |
| 25s 27s | BSI VS-NID, NATO restricted, EU Restrint (including 2nd Evaluation by NL) | 1:1 > 50.000h TE/TP | front 1U | | v2c/v3 | read-only | * * * * | , , | ,,, | ,,,, | ,,, | |
| 25s 27s |) | 1:1 > 50,000h TETTP | 1U 1 | * * * | v2c/v3 | read-only | ,,,, | , , | ,,, | ,,,, | ,,, | |
| 25s 27s | | > 50.000h TE/TP | front 1U | * * * | v2c/v3 | read-only | * * * * * | 、 、 | N 7 7 | ,,,, | ,,, | |
| 25s 27s | | 1:1 > 50.000h TE/TP | 1U 1-4 front | * * * | v2c/v3 | read-only | * * * * * | ~ ~ | N 7 7 | ,,,, | ,,, | |
| _ | *****BSI VS-NID, NATO restricted and EU Restrint planned/in preparation | | | | | | | - | | _ | | |

| Warranty Period (months) Warranty Coverage Parts & Work Basic Support (9 to 5, e-mail, phone) Software updates and upgrades Warranty Extension (per year) | List Proce Encryption funit (in €) Per external Key Server (in €): optional, no requirement Required Management Software 2-10 encryptors 11-25 encryptors 26-59 encryptors 51+ encryptors | Price | Key Management Group creation Group solation Key assignment Fall-over configuration | Certificate Authority & Management Certificate Creation Certificate Management | Device Management Device Diagnostics Link Monitoring (SNMP) Connection Diagnostics In-bant Network Diagnostics Remote Update/Upgrade | Management Access Identity-based access Identity-based authentication of user Number of hierarchy levels Number of roles Strict internal separation of users | Device Configuration Local (out-of-band) Remote (in-band) Remote (out-of-band) | Initial Device Set-up Local (out-of-band) Remote (out-of-band) | Management Software User Interface Native PC application Embedded Webapp CLI |
|---|---|-------|---|--|---|---|---|--|--|
| 24 on request on request on request | on request on request included included included | | **** | optional optional optional | | 、 G N 、 、 、 | 、、、 | , , | • • |
| 24 on request on request on request | on request on request included included included included | | **** | optional optional optional | **** | t on N t t | * * * | ,, | • • |
| 24 on request on request | on request on request included included included | | **** | optional optional optional | * * * * * | \$ 07 N \$ \$ | * * * | • • | • • |
| 24 on request on request | on request on request included included included included | | * * * * | optional optional optional | * * * * * | 5 07 N 5 5 | * * * | , , | 、、 |
| 24 on request on request on request | on request on request included included included included | | ,,,, | optional optional optional | ,,,,, | \$ 07 N \$ \$ | 、、、 | , , | |
| 24 on request on request on request | on request on request included included included included | | ,,,, | optional optional optional | ,,,,, | \$ 07 N \$ \$ | , , , | , , | |
| 24 on request on request on request | on request on request included included included | | ,,,, | optional optional optional | ,,,,, | (07 N) ((| ,,, | , , | |
| 24 on request on request on request | on request on request included included included included | | ,,,, | optional optional optional | ,,,,, | 5 on N 5 5 | 、、、 | * * | 、、、 |

| Ω |
|----|
| Ð |
| 3 |
| ລ |
| Ξ. |
| 8 |
| - |

| | | Cofenet CN/010 | Cofonat CNA030 | Cofenat CNR010 | Cofenet CNR100 | Cofenet CN9000 | Cafanat CN0100 | Cofenet CN0120 |
|---|---|-------------------|--|-----------------|-----------------|----------------------------------|--------------------|-------------------|
| Mark Mark <th< th=""><th>Line Interface/Supported Line Rates</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<> | Line Interface/Supported Line Rates | | | | | | | |
| And And one An | 10 Mbs 100 Mbs | < /RJ45 | <td><pre></pre></td> <td></td> <td></td> <td></td> <td></td> | <pre></pre> | | | | |
| Image: Part Property For Part Prope | 1 Gbps | ✔/RJ45 | ✓/SFP | ✓/RJ45/SFP | ✓/SFP | <td></td> <td></td> | | |
| Image: Part of the | 10 Gaps | | | | ✔/SFP | V/SFP+ | | |
| Matrix Matrix< | 25Gps | | | | | 577. | | |
| Note Sector Sector <td>40 Gbps</td> <td></td> <td></td> <td></td> <td></td> <td>V/SFP+</td> <td></td> <td></td> | 40 Gbps | | | | | V/SFP+ | | |
| Subset Subset Subset <t< td=""><td>In apps</td><td></td><td></td><td></td><td></td><td>VISEP+</td><td></td><td>VIJOPP-20</td></t<> | In apps | | | | | VISEP+ | | VIJOPP-20 |
| Metwork Topologie Methods Set Note Control Main Building Farmer Main Building Farmer Building F | Virtual Appliance | | | | | up to to calus at up to too each | | |
| rand gran gran and a set of the s | Sunnorted Network Tonologies | | | | | | | |
| Autor (PSP) Marcian (PSP) < | | | | | | | | |
| Intel Sector | Point-to-Point (P2MP) Point-to-Multipoint (P2MP) | , , | , , | , , | 、、 | , , | 、、 | , , |
| Index Enclose | Multipoint (MP) | ٢ | ٢ | ٢ | ٢ | ٢ | ٢ | ٢ |
| and Encode Private Une (EV-Lan) Encode Visual Private Une (EV-L | Supported Metro Ethernet Topologies | | | | | | | |
| Ander Encore house Live (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Encore house Live (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Ander Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Image: Constraint of the CV-LAN (EV-LAN) Image: Constrainton (EV-LAN) Image: Constraint of the CV- | Dorthogoad | | | | | | | |
| Enton Private Tre (EPFrame) Enton Private Tre (| | ٢ | ٢ | ٢ | ۲ | ٢ | ۲ | ۲ |
| Mode Environ E | Ethernet Private Tree (EP-Tree) | | . < | : ح | . < | . < | . < | |
| Med Event Vitual Finan Line (EVF-Line) X <thx< th=""> <thx< th=""> X</thx<></thx<> | | | | | | | | |
| Encred Virual Prace Trie (EPF-rice) Encred Virual Prace Trie (EPF-rice) Marsel | | | | | | | | |
| Control Control Control <td>Ethernet Virtual Private Line (EVP-Line)</td> <td>< र</td> <td></td> <td>((</td> <td>< <</td> <td></td> <td>< <</td> <td>, ,</td> | Ethernet Virtual Private Line (EVP-Line) | < र | | ((| < < | | < < | , , |
| Id Networks (Encryption) Id Networks (Encryption) Id Networks (Encryption and a second s | Ethernet Virtual Private LAN (EVP-LAN) | ۲, | ۲, | ς • | ۰ ، | ۲, | ۰ , | ۲, |
| a in FLS OED in FLS OED </td <td>Supported Networks (Encryption)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> | Supported Networks (Encryption) | | | | | | | |
| Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint Soft Mint | Ethernet | ¢ | ¢ | ¢ | <. | ¢ | ¢ | ¢ |
| ed Networks (Transport of Encrypted Frame) ed Networks (| MPLS (MPLSoE) IPv4/IPv6 | ٢ | ٢ | ٢ | ٢ | ٢ | ٢ | ٢ |
| id Networks (Transport of Encrypted Frame) if native a if native a if native a if opperative a | | | | | | | | |
| In used Image: Some as S | Supported Networks (Transport of Encrypted Frame) | | | | | | | |
| E-OMPLS Go TCP TCP < | Ethernet (native) | ٢ | ٢ | ٢ | ۲ | ٢ | ۲ | ٢ |
| TCP TCP | MPLS (EOMPLS) | ۰ ۲ | . ۲ | . ۲ | ۰ ۲ | ٢ | * Boardman 04 2017 | * Boadman 04 2017 |
| IUSec Scenarios Scenarios Foadmap 04 2017 ant Inade Inade Inade Inade Mainoand/Finware Inade Inade Inade Inade Mainoand/Finware Inade Inade Inade Inade Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas | | | | ٠ | | | * Roadmap Q4 2017 | * Roadmap Q4 2017 |
| I Usage Scenarios enant anat naged d encryption service d encryption service id encryption service Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas Senetas | UDP | | | | | | * Roadmap Q4 2017 | * Roadmap Q4 2017 |
| nant ant ant and anged anged decorption service decourtly service Mailoard/Finware Key Mangement Key Mangement Senetas/Senetas | Supported Usage Scenarios | | | | | | | |
| nant nage nage d encyption service d encyption | Single tenant | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ |
| naged de eoryption service de | Multi-tenant | | | | | ✓ /one tenant per port | | |
| nused Mainboard/Firmare Senetas:Senetas Senetas:Senetas Senetas:Senetas Senetas:Senetas Senetas:Senetas Senetas:Senetas Senetas:Senetas Senetas:Senetas Senetas Seneta | Self-managed | ۲ | ۲ | ٢ | ۲ | ۲ | ۲ | ۲ |
| n used Mairboard/Firmware Kev Monooment Senetas Seneta | Managed encryption service | ((| | ((| , , | | | |
| n used Mainboard/Firmware Kev Monooment Senetas/Senetas | manager sevening service | | | | | | | |
| Mainboard/Firmware Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/DQuantique Senetas/Senetas Senetas/DQuantique Senetas/Senetas Senetas Senatas Senetas Senatas Senetas Senatas Senetas Senat | Platform | | | | | | | |
| re Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/DQuantique Senetas/Senetas Senetas/DQuantique Senetas/Senetas Senetas Sentas Senetas Senetas Senetas Senetas Sentas Sentas Senetas Sentas S | | | | | | | | |
| | Mainboard/Firmware Kev Management | Senetas/Senetas | Senetas/Senetas | Senetas/Senetas | Senetas/Senetas | Senetas/IDQuantique | 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.

| Tunnel (Ethernet) over Ethernet) Max. number of VLAN IDs Max. number of VLAN IDs Integrity protection (agorithm) Authentication length (bytes) Hegiby yro flexiton Variable replay window (size) Counter length (in bytes) Frame overhead unauthenticated encryption Frame overhead unauthenticated encryption (AE) Ethernet multi-top support | Transport (Payload only) Max. number of peers Max. number of MAX Addresses Max. number of Max. Number of Max. Max. number of MAX Addresses Max. number of MAX Addresses Max. number of MAX Addresses Max. Adaptive encryption offset based on frame content. Ethernyse mutation Ethernyse mutation Frame overhead authenticated encryption (AE) Ethern timuli-top support | Encryption Modes Native Ethernet Encryption Frame Encryption (Bulk - P2P only) Integrity protection (algorithm) Integrity protection Authentication length (bytes) Replay protection Frame overhead (nuthenticated encryption) Ethernet multi-hop support Ethernet multi-hop support | Latency Latency P2P Mode out-through store & forward Latency MP Mode out-through store & forward | Processing Method au-through store&torward FPGA ASIC CPU | Data Plane Encryption Standard and Processing Encryption Standard Block Cipher Peteret Made of Operation Alternative Mode of Operation Key Length (in bit) | |
|--|--|--|--|---|---|--|
| 2 2 unlimited GCM 16 5 256 frames 5 8 (C/TR) 24 + trunel (min. 18 bytes) 24 + trunel (min. 18 bytes) | 512 4000/unimited 2:56 9:CM 16 2:56 frames 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | GCM 16 256 frames 8 (CTF) + turnel (min 18 bytes) 24 + turnel (min 18 bytes) | <10µs (@1Gbps) <10µs (@1Gbps) | \$. \$ | AES GCM CFB/CTFI 128/256 | |
| 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 4.000/unimited 226 GCM 16 226 frames 0 (CFB) / 8 2/4 (CTFt) 2/4 | GCM GCM GCM 16 16 256 frames 256 frames 8 (CTR) + tunnel (min 18 bytes) 24 + tunnel (min 18 bytes) 24 + tunnel (min 18 bytes) | <10//s (@1Gbps) <10//s (@1Gbps) | ۰ . ۲ | AES GCM CFB/CTR 128/256 | |
| 2 2 unlimited GCM 16 256 fames 5 8 (CTR) 24 + tunnel (min. 18 bytes) 24 + tunnel (min. 18 bytes) | 4000unlimited 256 3CM 16 256 fames 256 fames 0 (CFB) 8 (CTR) 24 | aCM | <10µs • • • | < · < | AES GCM CFB/CTR 128/256 | |
| 2 2 unlimited GOM 16 256 frames 5 8 (CTR) 24+ tunnel (min. 18 bytes) 24+ tunnel (min. 18 bytes) | 512 4000/uniinited 512 GCM 16 256 frames 5 5 5 5 6 (CFE) 8 (CTFI) 24 | GCM GCM 16 256 frames 8 (CTR) + turnel (min 18 bytes) 24+ turnel (min 18 bytes) | <548 •2548 | < · < | AES GCM CFB/CFR 128/256 | |
| | 512 4000/unlimited 512 16 8 CM 18 256 frames 5 6 C/FB/ 8 (CTR) 24 | | <5/18 | \$. \$ | AES GCM CFBCTH 128256 | |
| • Roadmap Q4 2017 * Roadmap | 4000unlimited 512 'GCM (Roadmap Q4 2017) 16 256 frames 5 5 6 (CTF) 8 (CTF) 24 | • Roadmap Q4 2017 | <2µs <2µs | × × | AES CTR GCM (Roadmap 04 2017) 128/256 | |
| • Readmap Q4 2017 | 4000/unihihid 512 -GCM (Readmap 04 2017) 16 256 frames 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | • Roadmap Q4 2017 | Srt& | ч ч | AES CTR GCM (Roadmap 04 2017) 128/256 | |
| | limitation only in MAC mod | | | | | |

* except for CN1910/CN1912 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.

| Traffic Flow Security | Traffic Masking | Based on VLAN ID and presence of MPLS tag MPLS EoIP IP | Based on presence of MPLS tag MPLS EoIP IP | Based on VLAN ID MPLS EoIP IP | Mixed Ethernet, MPLS, EoIP and IP Support | Based on MAC Address Based on VLAN ID Based on Futerype Based on Multicast Group Based on Presence of MPLS Tag Based on Presence of MPLS Tag Combination of multiple selection criteria | Selective Encryption | Transport/Tunnel Mode Mximum number of IP addresses Maximum number of IP addresses Maximum number of IP addresses Maximum number of IP addresses Maximum number of IP addresses Integrity protection Variable replay window (siza) Counter length (fn bytes) Packat overhead authenticated encryption (AE) | Supported IP versions IPv4 Supported Tanamission protocols TCP UDP | Native IP Encryption | Ethernet over IP (EoIP) Tunnel (Ethernet over IP) Supported transmission protocols (UDP/TCP) Max. number of parses Max. number of VLAN UBs Integrity protection Authentication length (bytes) Felaby protection Counter length (in bytes) Frame overhead authenticated encryption (AE) Ethernet multi-hop support |
|-----------------------|-----------------|---|---|--|---|---|----------------------|---|--|----------------------|--|
| 7 | | | | 2 | | , ,,,, | | | | | UDPTCP 2 unlimited GGM 16 226 fames 8 (CTR) + tunnel (min. 38 bytes) 24 + tunnel (min. 38 bytes) |
| ٩ | | | | ۲. | | 、 、、、、 | | | | | UDPTCP UDPTCP UDPTCP 2 unlimited unlimited unlimited unlimited unlimited unlimited unlimited unlimited GCM 16 16 256 frames 256 frames 256 frames 5 5 5 256 frames 2 24 + turnel (min. 38 bytes) 8 (CTFI) + turnel (min. 38 bytes) 8 (CTFI) + turnel (min. 38 bytes) |
| ۲ | | | | ۲, | | 、 、、、、 | | | | | UDP/TCP 2 unlimited GCM 16 256 frames 5 8 (CTR) + turnet (min .36 bytes) 24 + turnet (min .36 bytes) |
| ۲ | | | | ۲, | | , ,,,, | | | | | UDP/TCP 2 unlimited unlimited GCM 16 256 frames 5 8 (CTF)+ tunnel (min. 38 24 + tunnel (min. 38 bytes) |
| l | | | | ۲, | | 、 、、、、 | | | | | |
| Roadmap Q4 2017 | | | | ۲ | | 、 、、、、 | | | | | * Readmap Q4 2017 |
| Roadmap Q4 2017 | | | | ۲. | | , ,,,, | | | | | - Readmap Q4 2017 |

| Key Agreement and Key Exchange Master Key (KEK) Agreement Master Key (KEK) Exchange Protocol Automatic Change of Master Key Change (min) Separate Master Key (KEK) per site Separate Master Key (KEK) per group Sesion Key (DEK) Exchange Agreement Sesion Key (DEK) Exchange Agreement Sesion Key (DEK) Exchange Agreement Automatic Change of Sesion Keys Minimum Time Interval for Sesion Keys | Device Authentication Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encryptor Key length Maximum number of certificates per encryptor Key length Ad-hoc authentication of peers (manual) Signature key protocol | RSA Key length Elliptic Curve Cryptography (ECC) Key length Supported Curves: NIST Bairpool Custom Curves Hash Algorithms SHA:2 Key length | Auto-discovery of network encryptors Auto-discovery of New server Disabling of auto-discovery Key Server Integrated Key Server Support for external Key Server External Key Server Support for multiple distributed Key Server Support for infall-over to back-up Key Server Support for fall-over to back-up Key Server Autonomous operation Autonomous operation Key Generation and Storage Harrivae Random Kumber Generation Tamper Security Key Storage (tamper-evident or tamper-proof) Asymmetric Key Algorithms (Public Key Cryptography) | Auto-discovery |
|---|---|--|---|----------------|
| ATM F | 19 | | | |

| 7 | * * * * |
|---|-------------|
| | |
| < | **** |
| , | * * * * |
| | |
| ~ | |
| ۲ | **** |

| ,,,, | 512 | 2048 | телтр |
|-------|-----|------|-----------------|
| | 512 | 2048 | тегр |
| * * * | 512 | 2048 | телр |
| ,,, | 512 | 2048 | ТЕЛТР |
| ,,, | 512 | 2048 | ✔/ORNG TE/TP |
| ,,,, | 512 | 2048 | ✔ ORNG TE/TP |
| | 512 | 2048 | V/ORNG TE/TP |

| NIST SP800-56A | ATM Forum Security Specifications | ٢. | 1 440 | ٢ | Senetas | ECDH/RSA | ECDSA/RSA | x.509 64 512 (ECC)/2048 (RSA) |
|----------------|---|------|--------------|----|---------|----------|-----------|-------------------------------------|
| NIST SP800-56A | ATM Forum Security Specifications | ٩. | 1 440 | ٢ | Senetas | ECDH/RSA | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| NIST SP800-56A | ATM Forum Security Specifications | • • | 1 440 | ٢ | Senetas | ECDH/RSA | ECDSA/RSA | x.509 64 512 (ECC)/2048 (RSA) |
| NIST SP800-56A | ATM Forum Security Specifications ATM Forum Security Specifications ATM Forum Security Specifications ATM Forum Security Specifications | • • | 1 440 | ۲, | Senetas | ECDH/RSA | ECDSA/RSA | x.509 64 512 (ECC)/2048 (RSA) |
| NIST SP800-56A | ATM Forum Security Specifications | ٩. | 1 440 | ۲, | Senetas | ECDH/RSA | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| NIST SP800-56A | ATM Forum Security Specifications | ٩, ١ | 1 440 | ۲, | Senetas | ECDH/RSA | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| NIST SP800-56A | ATM Forum Security Specifications | ۲, | 1 440 | ٢ | Senetas | ECDH/RSA | ECDSAIRSA | x.509 64 512 (ECC)/2048 (RSA) |

| | 512 | ,, | |
|--|-----|-----|--|
| | 512 | , , | |
| | 512 | | |
| | 512 | • • | |
| | 512 | | |
| | 512 | , , | |

512

| Q | |
|----|--|
| Ω | |
| з. | |

| Group Key Distribution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAN ID Frames with MPLS tag IP Address IP Mutcast Group | Group Membership Definition Multicast group membership Individual membership Network membership VLAN membership Trunked VLAN membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multicast group Individual key per broadcast group (VLAN ID) | Key assignment based on: MAC address (pairwise and mixed) Multicast groups (mixed) VLAN ID (group) Port IP Address IP Multicast Group | Multipoint Key System Supported key systems: Painvee Group Miked (pairwise unicast, group multicast) | Key assignment based on: MAC Address VLAN ID Port Group IP Address | Point-to-Multipoint Key System Supported tey systems: Painvise Group | Key assignment based on: MAC Address ULAN ID Port Group IP Address | Point-to-Point Key System Supported key system Painvise Group | Key System |
|---|---|--|--|--|---|--|---|---|---|--|------------|
| , , | , , | , , , , | ٢ | 、 、 | **** | Bidirectional Group | ,,,, | S Bidirectional Group | ,,,, | Bidirectional Group | |
| | | *** * | ¢. | • • | **** | Bidirectional Group | **** | Sidirectional Group | **** | Bklirectional Group | |
| ~ ~ | | 、、、、、 | s, | 、 、 | * * * * * | Bidirectional Group | * * * * | Sidirectional Group | , , , , | Bidliectional Group | |
| , , | , , | , , , , | ۲, | , , | ,,,,, | Bidirectional Group | ,,,, | F Bidirectional Group | ,,,, | Sidirectional Group | Gemaito |
| , , | | , , , , | ۲. | | ,,,,, | Bidirectional Group | * * * * | S Bidirectional Group | * * * * | Sidirectional Group | |
| , , | | | ۲. | | ,,,,, | Bidirectional Group | ,,,, | S Bidirectional Group | ,,,, | Sidirectional Group | |
| ~ ~ | | , , , , | ٢ | • • | ,,,,, | Sidirectional Group | ,,,, | S Bidirectional Group | ,,,, | Sidirectional Group | |

| Boot Time Cold boot until operational (P2P) Warm boot until operational (P2P) | Security Approvals Safety Approvals | Height In 19" Rack Number of external encypted Ethernet ports Physical Device Access Redundant brieswer Supply Redundant, brieswappable power supply High Availability functionality (two-node cluster) MTBF Tamper Security | Event Log (oca) Audit Log (oca) Systog Support (Server) Unit | Logs | In-band Management SNMP (read-only/read-write) TLS Proprietary Remote Monitoring (SNMP) | Out-of-band Management Rs.2220/24 Separate Ethernet port Smart Card (Secure Card) Support USB Port | System Configuration and Management Access IP/4 IP/6 | Ehernet Fragmertation Point-to-Point Point-to-Multipoint Multipoint Dead Feer Detection Optical Loss Pass-Through Link Loss Carry Forward | Network Support Bump in the Wire deployment Junito Frame Support Ethernet Flow Control Via PAUSE |
|---|--|---|---|------|---|--|--|---|---|
| 65s 80s | FIPS140-2 L3, CC EAL2+, UC APL, NATO EN55022 class B, EN61000, ROHS | Desktop t back Readmap 2017 > 200000h TE/IP | | | RORW V1/A20V3 | , ,,, | | < < | |
| 65s 80s | FIPS140-213 CC EM.2+, UC API, NATO FIPS140-213 CC EM.2+, UC API, NATO FIPS140-213, CC EM.2+, UC API, N | Desktop t back Roadmap 2017 > 200.000 TE/TP | * * * | | RORW V1M2eV3 | | | * * * | |
| 65s 80s | FIPS140-2 L3, CC EAL2+, UC APL, NATO F EN55022 class B, EN61000, ROHS | 1U 1 front Readings 2017 > 200.000h 7E/TP | | | ROIRW | | | *** | |
| 65s 80s | FIPS140-2 L3, CC EAL2+, UC APL, NATO EN55022 class B, EN61000, ROHS | 10 1 front Readmap 2017 >20000h 7E/TP | | | ROIRW VIA2EM3 | | | * * * | * * |
| 65s 80s | FIPS140-2 L3, CC EAL2+ EN55022 class B, EN61000 ROHS | 4U 1-10 front Readmag 2017 > 100.000h TE/TP | * * * | | PO/RW VINZENS | < < < | | *** | |
| 65s 80s | FIPS140-2 L3/ CC EAL2+ in progress EN55022 class B, EN61000, ROHS | tu tont Readmap 2017 >200.0000 TE/TP | ,,,, | | RO/RW V1N2cV3 | | 、、 | , , , | , , |
| 65s 80s | EN55022 class B, EN61000, ROHS | tu front Nadimap 2017 > 200.00/h ∀£/IT₽/T₽ | *** | | ROPN V1/22043 | | | * * * | |

* 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

| Warranty Period (months) Warranty Coverage Parts Basi Basi Softe Warranty Extension (per year) | List Price Encryption Unit (in €) Per external Key Server (in €); Required Management Schware Optional SMC Sofware 5-10 5-10 11-20 unlimt | Key Management | Certificate Authority & Management Certificate Certificate | Device Management | Management Access | Device Configuration | Initial Device Set-up | User Interface |
|---|---|--|--|--|--|---|---|---|
| s) Parts & Work Basic Support (9 to 5, e-mail, phone) Software updates and upgrades ryear) | e List Price Encryption Unit (in €) Per extermal Key Server (in €); optional, no requirement, starting price Required Management Software Optional SMC Sofware 1-4 encryptors 5-10 encryptors 11-20 encryptors unlimited | Group creation Group isolation Key assignment Fall-over configuration | lanagement Certificate Creation Certificate Management | Device Diagnostics Link Monitoring (SNMP) Connection Diagnostics In-band Network Diagnostics Remote Update/Upgrade | Role-based access Identity-based authentication of user Number of hierarchy levels Number of roles Strict Internal separation of users | Local (out-of-band) Remote (in-band) Remote (out-of-band) | Local (out-of-band) Remote (out-of-band) | Native PC application Embedded Webapp CLI |
| 15% | on request ON7 included free on request on request on request | ,,,, | , , | ,,,,, | 2 3 (SMC)/4 (CM7) | ,,, | , , | , , |
| 15% ९ ९ ९ 12 | on request on request CM7 included free on request on request on request | , , , , , | , , | ,,,,, | 2 3 (SMC)/4 (CM7) | ,,, | , , | , , |
| 15 % < < < 12 | on request on request CM7 included free on request on request on request | ,,,, | , , | ,,,,, | 2 3 (SMC)/4 (CM7) | , , , | , , | , , |
| 15% 15% | on request on request CM7 included free on request on request on request | ,,,, | , , | ,,,,, | 2 3 (SMC)/4 (CM7) | ,,, | , , | , , |
| 15% 15% | on request on request CM7 included free on request on request on request | ,,,, | , , | ,,,,, | 2 3 (SMC)/4 (CM7) | , , , | , , | , , |
| 15% ९ ९ ९ 12 | on request on request CM7 included for request on request on request | ,,,, | , , | ,,,,, | 2 3 (SMC)/4 (CM7) | ,,, | , , | , , |
| ۲ <u>5</u> %% | on request ON7 included free on request on request on request | * * * * | | * * * * * | 2 3 (SMC)/4 (CM7) | • • • • | 、、 | 、、 |

| _ |
|----------|
| Q |
| 9 |
| <u> </u> |
| a |
| |
| = |
| <u>_</u> |
| <u> </u> |
| æ |

| * IP support only in combination with TRANSEC and limited to P2P. Additional overhead and latency. | Mainboard/Firmware Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas/Senetas Senetas | | Platform | د د | Self-managed C C C C C C C C C C C C C C C C C C C | | < | Supported Usage Scenarios | | Top | Ethemet (native) | Supported Networks (Transport of Encrypted Frame) | , | Ethemet < < < | Supported Networks (Encryption) | Ethernet Virtual Private Irve (EVP-Irve) | , , , , , , , , , , , , , , , , , , , | Ethernel Private LAN (FP-LAN) | < < | Supported Metro Ethernet Topologies | • | 22P) < < < < < < < < < < < < < < < < < < < | Supported Network Topologies | 100 Gbps | 40 Gbps | | a desire a second a s |
|--|--|---|----------|--------|--|------------------------|----|---------------------------|--|-------------------|------------------|---|---|---------------|---------------------------------|--|---------------------------------------|-------------------------------|-----|-------------------------------------|---|--|------------------------------|--|---------------------|--|---|
| overhead and latency. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Senetas/IDQuantique Senetas | | | ۲ | 、、 | ✓ /one tenant per port | ۲, | | | | 、、 | | , | . < | | | . < | 、、 | ۲ | | ۲ | , , | | ✓/SFP+ up to 10 cards at up to 10G each | <td></td> <td></td> | | |
| | Senetas/Senetas Senetas | i | | ۲ | , , | | ۲ | | * Roadmap Q4 2017 * Roadmap Q4 2017 | * Roadmap Q4 2017 | 、、 | | , | . < | | 、、 | | , , | ۲ | | ۲ | , , | | ✔/CFP-4 | | | |
| | Senetas/Senetas Senetas | | | ۲ | , , | | ۲, | | * Roadmap Q4 2017 | * Roadmap Q4 2017 | , , | | Ţ | | | , , | | , , | ۲ | | ۲ | , , | | ✔/QSFP-28 | | | |

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

| Tunnel (Ehernet) Max. number of MAC Addresses Max. number of MAC Addresses Max. number of VLAN Ds. Integrity protection (agorithm) Authentication sight (rytes) Repay protection Counter length vin Yow (size) Fame overhead authenticated encryption Fame overhead authenticated encryption (AE) Ehernet multi-top support | Transport (Payload only) Max. number of MAC Addresses Max. number of MAC Addresses Max. number of VAC Addresses Addresses Addresses Variable encryption offset (sed) Variable encryption offset based on frame content Entertype nutation Counter (anglift (in type) Counter (anglift (in type) Farme overhead untentimeticated encryption (AE) Enternet multi-hop support | Encryption Modes Native Ethernst Encryption Frame Encryption (Bulk - P2P only) Integrity protection (algorithm) Integrity protection Variable rapity window (size) Contrel ength (in bytea) Frame overhead (unauthenicitated oncryption) Enternet multi-hop support | Encryption Harowite FPGA ASIC CPU Latency Latency 2P Mode cut-through Latency VIP Mode cut-through cut-through stere & forward stere & forward | Processing Method cul-through store&torward | Data Plane Encryption Standard and Processing Encryption Standard Block Cipher Prefered Mode of Operation Alternative Mode of Operation Key Length (n. bh) |
|---|---|---|---|---|---|
| 2 untimited UCM 16 266 fames 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | 4000unimmed 256 900 910 910 910 910 910 910 910 910 910 | GCM 16 256 frames 5 8 (CTR) + turnel (min 18 bytes) 24 + turnel (min 18 bytes) | <(1078 (@.1090ba) <(0782 (@.1090ba) | | AES GCM GEBCTH 128/256 |
| 256 frames 5 8 (CTR) 24 + turnet (mn. 18 bytes) | 512 4000/unimited 256 6C:M 16 256 frames 5 5 0 (/CFB)/6 2.4 | GCM 16 266 frames 5 8 (CTR) + tunnel (rim 18 bytes) 24+ tunnel (rim 18 bytes) 24+ tunnel (rim 18 bytes) | <10µs (@10bps) <10µs (@10bps) | | AES GCM CFB/CTF 128/256 |
| • 2 untimited untimited CCM 16 266 frams 5 5 8 (CTR) 8 (CTR) 24 + turnes (min : 18 bytes) | 51 4000/uniined 256 COM 16 266 frames 266 frames 5 5 0 (CFB y 8 (CTF)) 24 | GCM 16 256 fames 5 8 (CTR) + turnel (min 18 bytes) 24 + turnel (min 18 bytes) | . clops • clops | | AES GCM CFB/CTR 128/256 |
| 2 unimited uccMi 16 256 fames 5 8 (CTR) 8 (CTR) 24 + tunnel (min. 18 bytes) | 512 4000/unined 512 90:00 16 256 transs 256 transs 5 0 (CFB)/ 8 (CTF) 2.4 | GCM 16 256 farmes 5 8 (CTR) + tunnel (min 18 bytes) 24 + tunnel (min 18 bytes) | • \$5 • \$5 | | AES GCM CFBCTR 138/256 |
| | 512 4000/uniined 512 802/M 16 256 transes 256 transes 5 5 0 (CFB)/ 8 (CTFb) 2 4 | | • \$5 • \$5 | | AES GCM CFB/CTR 128/226 |
| " Roadmap 04 2017 | 512 4000/unitrited 512 70 (Headmap 04 2017) 7 256 frames 5 5 8 (CTFR) 24 7 | * Foatmap 04 2017 | €Jus | ۲. | AES CTR GCM (Padamp 04 2017) 128/256 |
| • Roatmap 04 2017 | 512 4000/unitnitied 512 900/unitnitied 516 256 fames 5 5 8 (CTFF) 24 7 | • Roadmap O4 2017 | ene Ata | ۲. | AES CTR GCM (Roadmap C4 2017) 128/256 |
| | Irritation only in MAC mode | | | | |

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

Idquantique

| | Traffic Flow Security | Traffic Masking | Based on VLAN ID and presence of MPLS tag MPLS Epip IP | Based on preserve of MPLS tag MPLS EoIP IP | Based on VLAN ID MPLS Exp IP | Mixed Ethernet, MPLS, EoIP and IP Support | Based on IP Address Combination of multiple selection criteria | Based on NAC Address Based on YLN ID Based on Ethertype Based on Mutical Group Based on Mutical Group | Selective Encryption | Transport/Tunnel Mode Maimum number of peers Maximum number of in addresses Maximum number of multicast goups Integrity pottection (agorithm) Authentication leagth (bytes) Additional Authenticated Data (header) Replay Protection Variable replay window (size) Counter length (in bytes) Packet overhead authenticated encryption (AE) | Supported IP versions IP-4 Supported transmission protocols TCP UDP | Native IP Encryption | Ethernet over IP (EcIP) Tunnel (Ethernet over IP) Supported transmission protocols (UDP/TCP) Max. number of NAC Addresses Adtremication (algorithm) Septer protection (algorithm) Septer protection (Variable redue) (Variable re |
|--|-----------------------|-----------------|---|---|---------------------------------------|---|---|---|----------------------|--|---|----------------------|--|
| * EoIP only when using TRANSE(| ۶ | | | | ۲ | | ۶ | **** | | | | | UDP/TCP 2 unlimited unlimited CCM 16 256 frames 5 (CTR) + turnel (min. 38 bytes) 24 + turnel (min. 38 bytes) |
| EoIP only when using TRANSEC. Limited to P2P. Additional overhead and latency. | ٦ | | | | ۲ | | ۶ | ,,,, | | | | | UDP/TCP UDP/TCP UDP/TCP unimited unimited unimited unimited unimited unimited unimited unimited unimited GCM 16 16 256 frames 256 frames 256 frames 5 5 256 frames 256 frames 24+tume! (min. 38 bytes) 8 (CTR) + tume! (min. 38 bytes) 8 (CTR) + tume! (min. 38 bytes) |
| and latency. | ۲ | | | | ۲ | | ۲ | * * * * | | | | | UDP/TCP 2 unlimited unimited GCM 16 256 frames 256 frames 5 5 3 (CTF) + tunnel (min. 38 bytes) 24 + tunnel (min. 38 bytes) |
| | ۲ | | | | ۲ | | ۲ | * * * * | | | | | UDP/TCP 2 unimited unimited GCM 16 256 frames 8 (CTR) + turnel (min. 38 24 + turnel (min. 38 bytes) |
| | | | | | ۲ | | ۲ | * * * * | | | | | |
| | Roadmap Q4 2017 | | | | ۲ | | ٢ | * * * * | | | | | • Readmap O4 2017 |
| | Roadmap Q4 2017 | | | | ۲ | | ۲ | * * * * | | | | | • Readmap Q4 2017 |

Idquantique

| separate Master Key (KEK) per group Separate Master Key (KEK) per group Sesson Key (DEK) Exchange Agreement Sesson Key (DEK) Exchange Procool Automate Change of Sesson Keys Minimum The Interval for Sesson Keys | Key Agreement and Key Exchange Master Key (KEK) Agreement Master Key (KEK) Exchange Protocol Automatis Change of Master Key Automatis Change of Master Key | Ad-hoc authentication of peers (manual) Signature key protocol | Asymmetric Signature: Certificate Maximum number of certificates per encryptor Key length | Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encyptor Key length | Device Authentication | SHA-2 Key length | Hash Algorithms | Supported Curves: NIST Brainpool Custom Curves | Key length | Elliptic Curve Cryptography (ECC) | RSA Key length | Asymmetric Key Algorithms (Public Key Cryptography) | Hardware Random Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) | Key Generation and Storage | Key Management | Autonomous operation | e zarnativery server Support for fail-over to back-up Key Server Support for fail-over to back-up Key Server | Integrated Key Server Support for external Key Server | Key Server | Auto-discovery of v LANS Disabling of auto-discovery | Auto-discovery of intervious encyptions Auto-discovery of key servers | |
|--|--|---|---|--|-----------------------|------------------|-----------------|---|------------|-----------------------------------|----------------|---|---|----------------------------|----------------|----------------------|--|--|------------|---|--|--|
| ATMF | | | | | | | | | | | | | | | | | | | | | | |

| ۲ | 、、、、、 | * * * * | |
|---|---------|---------|--|
| ٢ | ** ** | | |
| ٢ | * * * * | * * * * | |
| ۶ | 、、、、、 | * * * * | |
| ۶ | 、、、、 | * * * * | |
| ۶ | 、、、、、 | * * * * | |
| ۲ | ,, ,, | | |

| ۲ ۲ | ۲ | 512 | 2048 | ТЕЛГР |
|-----|---|-----|------|-----------------|
| ۰ ۲ | ۲ | 512 | 2048 | телгр |
| ۰ ۲ | ۲ | 512 | 2048 | тетр |
| 、、 | ۲ | 512 | 2048 | ТЕЛТР |
| ۰ ۲ | ۲ | 512 | 2048 | ✔/QRNG TE/TP |
| ۰ ۲ | ۲ | 512 | 2048 | ✓ ORNG TE/TP |
| 、、 | ۲ | 512 | 2048 | V/ORNG TE/TP |
| | | | | |

| • ر | ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Senetas 1440 | ECDSAIRSA | x.509 64 512 (ECC)/Z048 (RSA) |
|-----|--|-------------------------------|-----------|-------------------------------------|
| ۲, | ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Senetas 1440 | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| ۰, | ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Serretas 1440 | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| ۲, | ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Servetas 1440 | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| ۲. | ATM Forum Security Specifications NIST SP800-56A | ECDH/IRSA Serietas 1440 | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| ۲. | ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Serretas 1440 | ECDSA/RSA | x 509 64 512 (ECC)/2048 (RSA) |
| 、 | ATM Forum Security Specifications ATM Fo | ECDH/RSA Senetas 1440 | ECDSAIRSA | x 509 64 512 (ECC)/2048 (RSA) |

| * * * | 512 | 2048 |
|-------|-----|------|
| ,,, | 512 | 2048 |
| ,,,, | 512 | 2048 |
| ,,, | 512 | 2048 |
| ,,, | 512 | 2048 |

| ~ | |
|---|--|
| ă | |
| S | |
| ä | |
| | |
| ę | |
| ē | |

Auto-disc

| Group Key Distribution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAN ID Frames with MPLS tag IP Address IP Address IP Mulcast Group | Goup Membership Definition Multicast group membership Individual membership Network membership VLAN membership Trunked VLAN membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multicast group Individual key per broadcast group (VLAN ID) | Key assignment based on: McC actress (panvise and mixed) Multicast groups (mixed) VLAN ID (group) Port Group (group) IP Address IP Multicast Group | Multipoint Key System Supported key systems: Painvise Group Mixed (pairwise unicast, group multicast) | Key assignment based on: NAC 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 | Point-to-Point Key System Supported key system Paint/se Group | Key System |
|---|---|---|--|--|---|---|---|---|---|--|--------------|
| , , | | *** * | ۲ | , , | ***** | Bidirectional Group | ,,,, | S Bidirectional Group | ,,,, | Bidirectional Group | |
| | | **** | c. | | **** | Bidirectional Group | **** | Skilrectional Group | **** | Skilrectional Group | |
| | | 、、、、、、 | ٢ | 、 、 | **** | Bidnectional Group | | Sidirectional Group | | Sidnectional Group | |
| , , | , , | , , , , | ۲ | , , | ,,,,, | Bidirectional Group | ,,,, | Sidirectional Group | ,,,, | Sidirectional Group | Iuquaiiiique |
| , , | | , , , , | ۲ | | **** | Ridirectional Group | ,,,, | State Control Circup | ,,,, | Bidirectional Group | |
| , , | | , , , , | ۲ | | **** | Bidirectional Group | * * * * | Sidirectional Group | ,,,, | Bidirectional Group | |
| , , | | , , , , | ۲, | | **** | Sidirectional Group | * * * * | Bidirectional Group | * * * * | Sidirectional Group | |

Idquantique

| ā | |
|----|--|
| ą | |
| La | |
| 크 | |
| ä | |
| L. | |
| Φ | |

| Boot Time Cold boot until operational (P2P) Warm boot until operational (P2P) | Security Approvals Satety Approvals | Height in 19 Rack Number of external encrypted Ethernet ports Physical Device Access Redundant Fewer Supply Reference and the wappable power supply High Availability functionality (two-node cluster) MTBF Tamper Security | Systeg Support (server) Unit | Logs Event log (local) Audit loc (local) | In-band Management SNM (read-only/read-write) TLS Foprieary Remote Montoring (SNMP) | IP-4 IPv6 Out-of-band Management IRS-232/V.24 Separate Ethernet port Smert Card (Secure Card) Support USB Port | Dead Peer Deerdon Optical Loss Pass-Through Link Loss Cany Forward System Configuration and Management Access | Network Support Bump in the Wire deployment Jurbo Frame Support Ethernet Fragmentation/Defragmentation Point-to-Point Point-to-Point Multipoint |
|---|--|--|---------------------------------|--|---|--|--|---|
| 65s 80s | FIPS140-2 L3, CC EAL2+, UC APL, NATO EN55022 class B, EN61000, ROHS | Desktop 1 back Readmap 2017 > 200000h TE/TP | . . | ς ς | ROIRW V1N2cv3 | < <<< << | , , | |
| 65s 80s | FIPS140-213, OC EAL2+, UC APL, NATO FIPS140-213, OC EAL2+, UC APL, | Deskop I beck Roadmap 2017 > 200.000h TE/TP | ج - | | ROIRW V1/A2dV3 | < < < < < | * * * * | , , |
| 65s 80s | FIPS140-2 L3, CC EAL2+, UC APL, NATO F EN55022 class B, EN61000, ROHS | 1U 1 front Reading 2017 > 200000h TE/TP | ۲. | | ROIRNV V1/A2cW3 | < < < < | *** | * * |
| 65s 80s | =IPS140-2 L3, CC EAL2+, UC APL, NATO E N55022 class B, EN61000, ROHS | ۲۵ ۲۵۲ ۲۵۵۳ ۲۵۵۳ ۲€/۲P | ~ · | | PO JAW | < < < < | * * * | |
| 65s 80s | FIPS140-2 L3, CC EAL2+ EN55022 class B, EN61000 ROHS | 4U 1-10 Nonima 2017 > 100.000h TE/TP | . . | | PO PR | < < < < | | |
| 65s 80s | FIPS140-2 L3/ CC EAL2+ in progress EN55022 class B, EN61000, ROHS | ru + tor Reading 2017 > 200 000h TE/TP | < · | | ROIAN VINZOV3 | < < < < | | |
| 65s 80s | EN55022 class B, EN61000, ROHS | 10 1 tron1 Reading 2017 > 20 cooh 1ETP | . . | ς ς | RO FW | x x x x | | * * |

* 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

| 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) | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ |
| Management Access | | | | | | | | |
| | Role-based access | , , | , , | , , | , , | , , | , , | , , |
| | Number of hierarchy levels | ∾ ' | 22 | 22 | 22 | 22 | 0 | 10 |
| | Number of roles | 3 (SMC)/4 (CM7) |
| | Strict internal separation of users | ۲ | ۲ | ۲ | ۲ | ۲ | ۰, | ۲ |
| Device Management | | | | | | | | |
| | Link Manitoring (SNIMB) | (م | (م | : ۲ | : ۲ | : ۲ | | |
| | Connection Diagnostics | ۹ ، | ۹ ، | ۲, | ۹ ، | ۰, | ۰ ، | ۰ ، |
| | In-band Network Diagnostics | <i>, ,</i> | <i>、、</i> | ((| <i>、、</i> | < र | | र र |
| | 100 | | | | | | | |
| Certificate Authority & Management Certificate | lanagement Certificate Creation | ۲ | ٢ | ٢ | ٢ | ٢ | ۲, | ٢ |
| | Certificate Management | ۲ | ۲ | ۲ | ۲ | ۲ | ۲, | ۲, |
| Key Management | | | | | | | | |
| | Group creation | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ |
| | Group isolation | ٢ | ٢ | ٢ | ٢ | ٢ | ۲, | ۲, |
| | East continuation | (م | (م | : <i>۲</i> | (م | : <i>۲</i> | : ۲ | : ۲ |
| | | | • | | • | • | | |
| Price | | | | | | | | |
| List Price Encryption Unit (in €) | H/In €) | on request |
| Per extermal Key Server | Per extermal Key Server (in €); optional, no requirement, starting price | on request |
| Required Management Software | Software | CM7 included |
| Optional SMC Sofware | 1-4 encryptors | free |
| | 5-10 encryptors | on request |
| | i i-co encryptions unlimited | on request |
| | | | | | | | | |
| Warranty Period (months) | s) | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| warranty Coverage | Parts & Work | | | | | | | |
| | Software updates and upgrades | < • | < • | ۰ ، | < • | ۰ ، | 、、 | 、、 |
| Warranty Extension (per year) | year) . | 10% | 10% | 10% | 10% | 10% | 10% | 10% |

| | Rohde & Schwarz Rohde & Schwarz | Rohde & Schwarz Rohde & Schwarz | Rohde & Schwarz Rohde & Schwarz | Rohde & Schwarz Rohde & Schwarz | Platform used Mainboard/Firmware Key Management |
|---|------------------------------------|--|---|------------------------------------|--|
| | | | | | Platform |
| separate network and security management (NMS, SMS) | , , , | ,,, | , , , | | Self-managed Managed encryption service Managed security service |
| | ۲ | 2 | 7 | ۲ | Single tenant Multi-tenant |
| | | | | | Supported Usage Scenarios |
| supported by STIline IP Roadmap O3 2017 supported by STIline IP Roadmap O3 2017 supported by STIline IP Roadmap O3 2017 | | , , | , , | | Ethernet (rative) MPLS (EoMPLS) IP-4/IP-6 TCP UDP |
| | | | | | Supported Networks (Transport of Encrypted Frame) |
| supported by SITline IP Roadmap Q3 2017 supported by SITline IP Roadmap Q3 2017 | ۲ | ۲ | , | ٢ | Ethernet MPLS IPv4/IPv6 |
| | | | | | Supported Networks (Encryption) |
| | * * * | ,,, | , , , | | VLAN-based Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private Tree (EVP-Tree) Ethernet Virtual Private LAN (EVP-LAN) |
| | * * * | , , , | , , , | | Port-based Ethernet Private Line (EP-Line) Ethernet Private Line (EP-Tree) Ethernet Private LAN (EP-LAN) |
| | | | | | Supported Metro Ethernet Topologies |
| | 、、、 | , , , | ,,, | • • • • | Point-to-Point (P2P) Point-to-Multipoint (P2MP) Multipoint (MP) |
| | | | | | Supported Network Topologies |
| | | | | | Virtual Appliance |
| lserba uo | ✓ /mR45/4xSFP+ ✓ /OSFP | ✓ /4XR.4/45/4XSFP+ ✓ /4XR.4/45/4XSFP+ ✓ /4XR.4/45/4XSFP+ ✓ /4XR.4/45/4XSFP+ | ✓/4xRJ45/4xSFP ✓/4xRJ45/4xSFP ✓/4xRJ45/4xSFP ⊄/(‰anse upgrade) | ₹.RJ45 %RJ45 | 10 Mbs 100 Mps 1 Gbps 10 Gbps 25 Gps 40 Gbps 100 Gbps |
| - | | | | | Line Interface/Supported Line Rates |
| | SITLine ETH40G | SITLine ETH10G | SITLine ETH4G | SITLine ETH50 | |
| | | rz Cybersecurity | Rohde & Schwarz Cybersecurity | | |

| Tunnel (Ethernet) Max. number of paers Max. number of MAC: Addresses Max. number of VLAN IDS Integrity potection (egothm) Authentication length (bytes) Replay protection Variable replay window (size) Counter length (in bytes) Frame overhead unauthenticated encryption Frame overhead unauthenticated encryption (AE) Ethernet multi-hop support | Transport (Payload only) Max. number of pages Max. number of MAC Addresses Max. number of VLAN IDs Integrity protection (agorithm) Authentication length (bytes) Replay protection Variable encryption offset Variable encryption offset Adaptive encryption offset Adaptive encryption offset Adaptive encryption offset Entertype mutation (unauthenticated encryption only) Frame overhead unauthenticated encryption Frame overhead authenticated encryption (AE) Etherne tmult-hop support | Latency Latency Latency Latency P2P Mode cut-through store & forward Latency MP Mode cut-through store & forward Encryption Modes Native Ethernet Encryption Frame Encryption (Buik - P2P only) Integrity protection Authentication length (bytes) Frame voethead (mathemicated encryption) Frame overhead (authenticated encryption) | Processing Method Curryption Standard and Processing Encryption Standard Block Cipher Preferred Mode of Operation Alternative Mode of Operation Method Processing Method cut-through store&forward Encryption Hardware FPGA ASIC FPGA ASIC |
|--|--|---|---|
| 2.50 unimited 2.50 GCM 8.16 3.framss.per.priority 5. 20 18-26 (P2P), 28-36 (MP) | 2.50 uniimted 2.50 GCM 8-16 3 frames per priority 5 (PP) 10 (MP) 13-21 (PP), 16-26 (MP) | · va · va | C S S S S S S S S S S S S S S S S S S S |
| 4000 uninnied 4000 GCM 8-16 3 frames per priority 5 5 25 25 25 25 | 4000 unlimited 4000 GCM 8-16 3 frames per priority 5 (PP) 10 (MP) 13-21 (PP), 18-26 (MP) | S4s 5,s 6CM 8 CM 8 CM 8 CM 8 CM 8 CM 8 CM 8 CM 9 CCFB), 5 13-21 13-21 | Rohde & Schwa |
| 4000 uninined 4000 GCM 8-16 3 frames per priority 5 18-26 P2P 28-36 (MP) | 4000 unlinted 4000 GCM 8-16 3 Itames per priority 5 (PP) 10 (MP) 13-21 (PP), 18-26 (MP) | جابہ جابع GCM ج BCM عباق BCM BCM Share BCM Shar | Rohde & Schwarz Cybersecurity |
| 4000 unininied 4000 GCM 8-16 3 frames per priority 5 2 18-26 (PSP), 28-36 (MP) | 4000 uniimhed 4000 GCM 8-16 3 Irames per priority 5 (PP) 10 (MP) 13-21 (PP), 18-26 (MP) | جلاه د د د د د د د د د د د د د د د د د د د | C C S S S S S S S S S S S S S S S S S S |
| turnel in multipoint mode only replaces destination address | | dependent on packet size/bandwidth | |

| Traffic Flow Security | Traffic Masking | Based on VLAN ID and presence of MPLS tag MPLS EolP | Based on presence of MPLS tag MPLS EoIP IP | Based on VLANID MPLS Eolp | Mixed Ethernet, MPLS, EoIP and IP Support | Based on MAC Address Based on VLAN ID Based on Furtypon Based on Multicast Group Based on Parence of MPL/S Tag Based on IP Ardress Based on IP Ardress Combination of multiple selection ortieria | Selective Encryption | Morinum number of peak Maximum number of In addresses Maximum number of multicast groups Integrity potection (adjorithm) Authentication erght (rytes) Additional Authenticated Data (freader) Replay Protection Variable registy window (size) Counter length (in bytes) Packet overhead authenticated encryption (AE) | Transport/Tunnel Mode | Supported transmission protocols TCP UDP | Supported IP versions IP v4 IP v6 | Native IP Encryption | Ethernet over IP (EoIP) Tunnel (Ethernet over IP) Supported transmission protocols (UDP/TCP) Max. number of typens Max. number of VIAN UDs Integrity protection (algorithm) Authentication terrgit (bytes) Replay protection Variable reply window (size) Counter length (h bytes) Frame overhead unauthenticated encryption Frame o | |
|-----------------------|-----------------|---|---|---------------------------------|---|--|----------------------|---|---|--|--|----------------------|--|-------------------------------|
| | | | | | | , ,,,, | | | | | | | | |
| | | | | | | < <<< | | | | | | | | Rohde & Schwa |
| | | | | | | < < < < < | | | | | | | | Rohde & Schwarz Cybersecurity |
| | | | | | | , ,,,, | | | | (6. (6 | 0.0 | | | |
| | | | | | | | | | supported by SITline IP Roadmap Q3 2017 | supported by SITTline IP Roadmap Q3 2017 supported by SITTline IP Roadmap Q3 2017 | supported by SITTline IP Roadmap Q3 2017 supported by SITTline IP Roadmap Q3 2017 | | | |

| Session Key (DEK) Exchange Agreement Session Key (DEK) Exchange Protocol Automatic Change of Session Keys Minimum Time Interval for Session Key Change (min) | Master Key (KEK) Agreement Master Key (KEK) Exchange Protocol Automatic Change of Master Key Minimum suggested Time Interval for Master Key Change (min) Separate Master Key (KEK) per site Separate Master Key (KEK) per group | Key Agreement and Key Exchange | Ad-hoc authentication of peers (manual) Signature key protocol | Asymmetric Signature: Certificate Maximum number of certificates per encryptor Key lenght | Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encryptor Key length | Device Authentication | SHA-2 Key length | Hash Algorithms | Supported Curves: NIST Brainpool Custom Curves | Elliptic Curve Cryptography (ECC) Key length | RSA Key length | Asymmetric Key Algorithms (Public Key Cryptography) | Hardware Flandom Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) | Key Generation and Storage | Key Management | Autonomous operation | s nueva work very server Stupport for external Key Server External Key Server Support for rtail-over to back-up Key Server Support for fail-over to back-up Key Server | Key Server | Auto-discovery of larvoire in Laypuns Auto-discovery of key servers Auto-discovery of VLANs Disabling of auto-discovery | Auto-discovery |
|---|--|--------------------------------|---|---|---|-----------------------|------------------|-----------------|---|---|-------------------|---|--|----------------------------|----------------|----------------------|--|------------|--|----------------|
| Rohde & Schwarz Rohde & Schwarz 1 | DHECKAS | | ECDSA | x.509 1 257 | | | 256 | | ٢ | 257 | 2048 | | ✔ (PTG-3) TE/TP | | | ۲ | ₹, , | | < < < < | |
| Rohde & Schwarz Rohde & Schwarz | DH-ECKAS | | ECDSA | x 509 1 257 | | | 256 | | ۲ | 257 | 2048 | | ✔ (РТG-3) ТЕ/ТР | | | ۲ | N | | • • • • | |
| Rohde & Schwarz Rohde & Schwarz | ECDH Seo | | ECDSA | x.509 1 257 | | | 256 | | ۲ | 257 | 2048 | | ✔ (РТС-3) ТЕ/ГР | | | ۲ | ₹ ₹ \$ | | < < < < | |
| Rohde & Schwarz Rohde & Schwarz | CDHECKAS | | ECDSA | x.509 1 257 | | | 256 | | ۲ | 257 | 2048 | | ✔ (PTG-3) TE/TP | | | ۲ | N K K | | < < < < | |
| | | | | | | | | | | | | | | | | | | | Automatische Partnersuche über VLANs | - |

Rohde & Schwarz Cybersecurity

| Group Key Dehrbution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAW ID Fannes with MPLS bg IP Address IP Mulicast Group | Group Membership Deinkion Mutilicasti group membership Individual membership VLAN membership Turimead VLAN membership IP Address | Group Key System Specifics Additional separate authenitation per group | Individual key per multicast group Individual key per broadcast group (VLAN ID) | Key assignment based on: Multicast groups (mixed) Multicast groups (mixed) VLAN ID (group) Port Group (group) IP Address IP Multicast (Group | Supported key systems: Gorup Maxed (pairwise unicast, group mulicast) | Multipoint Key System | Key assignment based on: VANC Address VAND Port Group IP Address | Supported key systems: Painvise Group | Port Group IP Address Point-to-Multipoint Key System | Group Key assignment based on: MAC Address VLAN ID | Supported key system Pairwise | Point-to-Point Key System | Key System |
|---|--|---|---|--|---|---|-----------------------|---|---|---|---|----------------------------------|---------------------------|-------------------------------|
| ۲. | , , | **** | ۲ | , , | *** | Unidirectional Group | | x | ٢ | ۲ | 、 | ۲ | | |
| 2 | ,, | ,,,, | ۲ | , , | ,,, | Unidirectional Group | | 2 | ۲ | | , | ۲ | | Rohde & Schwarz Cybersecurity |
| ۲ | , , | ,,,, | ۲ | , , | ,,, | Unidirectional Group | | ۲. | ٢ | ۰, | 、 | ۲ | | rz Cybersecurity |
| e. | , , | **** | ۲. | | * * * | Unidirectional Group | | ۲ | 5 | ۲ | • | ۲ | | |

| Boot Time Cold boot until operational (P2P) Warm boot until operational (P2P) | Security Approvals Safety Approvals | Height in 19" Rack Number of external encrypted Ethernet ports Physical Device Access Redundant Power Supply Redundant, hot-swappable power supply High Availability functionality (two-node cluster) MTBF Tamper Security | Logs Event Log (local) Audit.Log (local) Syslog Support (Server) Unit | Point-to-Multipoint Multipoint Dead Peer Detection Optical Loss Carry Forward IPv4 IPv6 Out-of-band Management Smart Card (Secure Card) Support USB Port In-band Management SSH SIMP (read-only/read-write) TLS Proprietary Remote Monitoring (SNMP) | Network Support Bump in the Wire deployment Jumbo Frame Support Ethernet From Control via PAUSE Ethernet Fragmentation/Defragmentation Point-to-Point |
|---|--|---|---|--|--|
| 60s | BSI VS-NfD, EU restreint CE, ROHS | 1U (1/2 19" width) front 1-1 350000h TE/TP | | × · · · · · · · · · · · · · · · · · · · | * * * |
| 40s 40s | BSI VS-NfD, EU restreint CE, ROHS | 1 1 or 4 front 1-1 170000h TE/TP | | si si si si si si si si si si si si si s | |
| 40s | BSI VS-NfD, EU restreint, **CC EAL44 CE, ROHS | 1 1 or 4 front 1-1 170000h TE/TP | | 5755 5755 5755 5755 575 575 575 575 575 | |
| 40s | BSIVS-NID, EU restreint, "CC EAL4+ BSIVS-NID, EU restreint, "CC EAL4+ CC EAL 4+ pending CE, ROHS CE, ROHS | 1 or 4 front 1-1 170000h | | | , , , |
| | CC EAL 4+ pending | | | | bis 16000 Bytes |

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity

| Warranty Extension (per year) | | | Warranty Coverage | Warranty Period (months) | | | | | Required Management Software | Per extermal Key Server (in €) | List Price Encryption Unit (in €) | Price | | | | | | Kev Management | | | Certificate Authority & Management | | | | | Device Management | | | | | Management Access | | | Device Configuration | | Initial Device Set-up | | | User Interface | Management Software |
|-------------------------------|-------------------------------|---------------------------------------|-------------------|--------------------------|----------------|------------------|------------------|-----------------|------------------------------|--------------------------------|-----------------------------------|-------|---|-------------------------|----------------|--------------------|----------------|----------------|------------------------|----------------------|------------------------------------|-----------------------|-----------------------------|------------------------|------------------------|-------------------|-------------------------------------|--------------------|----------------------------|--|-------------------|----------------------|------------------|----------------------|---|-----------------------|-----|-----------------|-----------------------|---------------------|
| r year) | Software updates and upgrades | Basic Support (9 to 5, e-mail, phone) | Parts & Work | (Sr | 51+ encryptors | 26-50 encryptors | 11-25 encryptors | 2-10 encryptors | Software | m (in €) | nit (in £) | | | Fail-over configuration | Key assignment | Group isolation | Group creation | | Certificate Management | Certificate Creation | Aan age ment | Remote Update/Upgrade | In-band Network Diagnostics | Connection Diagnostics | Link Monitoring (SNMP) | | Strict internal separation of users | Number of roles | Number of hierarchy levels | Role-based access Identity-based authentication of user | | Remote (out-of-band) | Remote (in-band) | Local (out-of-band) | Local (out-or-band) Remote (out-of-band) | | CLI | Embedded Webapp | Native PC application | Ø |
| 5% | 3% | 3% | ۲, | 12 | on request | on request | on request | on request | on request | on readout to | On regulast | | | ۲, | ۲, | ۶ | ٢ | | ۶ | ۲, | | ٢ | ۲ | ٢, | 、、 | | ٢ | 8 | N | 、、 | | ٢ | ٢, | ۲, | < | | ۲ | | < | |
| 5% | 3% | 3% | ۲ | 12 | on request | on request | on request | on request | on request | on reducer | on regulast | | | ٢ | ۰, | ٢ | ۲ | | ۲ | ۲ | | ٢ | ۲ | ۲, | , , | | ٩ | 8 | 2 | 、、 | | ٩ | ٢. | ۲ | ۲ | | ٢ | | ۲. | |
| 5% | 3% | 3% | ۲ | 12 | on request | on request | on request | on request | on request | on request | on regulast | | | ۲ | ۲, | ٢ | ۲ | | ۲ | ۲ | | ٢ | ۲ | ۲, | , , | | ٩ | 8 | 2 | 、、 | | ٢ | ۲, | ٢ | ۲ | | ٢ | | ۲. | |
| 5% | 3% | 3% | ۲ | 12 | on request | on request | on request | on request | on request | on redocat | on regulast | | | ۲ | ۲, | ٢ | ۲ | | ۲ | ۲ | | ٢ | ۲ | ۲, | , , | | ٩ | 8 | 2 | , , | | ٢ | ٩. | ¢, | ۲ | | ۲ | | ۲. | |
| | | | | | | | | | | | | | • | | | via key management | | | | | | | | | | | | customizable roles | | | | | | | | | | | | - |

© 2007 - 2017 Christoph Jaggi ALL RIGHTS RESERVED Absolutely no re-publishing, distribution or file modification without prior written consent of the author

| Platform Platform used Mainboard/Firmware Key Management | Self-managed Managed encryption service Managed security service | Supported Usage Scenarios Single tenant Mult-tenant | Ethernet (native) MPLS (EcMPLS) IPv4/IPv6 TCP UDP | Supported Networks (Transport of Encrypted Frame) | Ethernet MPLS IP v4A6 | Supported Networks (Encryption) | VLAN-based Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private Tree (EVP-Tree) Ethernet Virtual Private LAN (EVP-LAN) | Port-based Ethernet Private Line (EP-Line) Ethernet Private Tree (EP-Tree) Ethernet Private LAN (EP-LAN) | Supported Metro Ethernet Topologies | Point-to-Point (P2P) Point-to-Multipoint (P2MP) Multipoint (MP) | Supported Network Topologies | Virtual Appliance | 1 Gibps 10 Gibps 25Gps 40 Gibps 100 Gibps | 10 Mbs | Line interrace/supported Line Hates | | |
|---|--|---|--|---|-----------------------------|---------------------------------|--|---|-------------------------------------|---|------------------------------|-------------------|---|-----------------------------------|-------------------------------------|-------------|---------|
| atmedia/atmedia atmedia | | | ,,,,, | | , , , | | | | | 、、、 | | | R.145 | /RJ45 | | 50M compact | |
| atmedia/atmedia atmedia | | | ,,,,, | | , , , | | | | | < < < | | | ✓ IR445 | <td></td> <td>100M</td> <td></td> | | 100M | |
| atmedia/atmedia atmedia | * * * | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | | , , , | | | , , , | | | | | ✓ SFP ✓ SFP | ✓/SFP | | 16 | Secunet |
| atmedia/atmedia atmedia | * * * | | * * * * * | | , , , | | | | | | | | V.SFP+ V.SFP+ | COED. | | 10G | Inet |
| atmedia/atmedia atmedia | * * * | | * * * * * | | , , , | | | | | | | | V/QSFP V/QSFP V/QSFP | | Roadmap Q2 2017 F | 40G | |
| atmedia atmedia | | | * * * * * | | ,,, | | | | | , , , | | | ✔/QSFP28 ✔/QSFP28 ✔/QSFP28 ✔/QSFP28 | | Roadmap Q4 2017 | 100G | |

| Ethernet multi-hop support | Frame overhead unauthenticated encryption | Counter length (in bytes) | Variable replay window (size) | Autnentication length (bytes) | Integrity protection (algorithm) | Max. number of VLAN IDs | Max. number of MAC Addresses | Max. number of peers | Tunnel (Ethernet over Ethernet) | Ethernet multi-hop support | Frame overhead authenticated encryption (AF) | Frame overhead insuthenticated econotion | Counter langth (in botos) | Adaptive encryption onset based on traine content | Variable encryption offset | Definable encryption offset (fixed) | Variable replay window (size) | Replay protection | Authentication length (bytes) | Integrity protection (algorithm) | Max. number of VLAN IDs | Max number of MAC Addresses | ransport (Payload only) Max, number of neers | Hospital (Decideration) | Ethernet multi-nop support | Frame overhead (authenticated encryption) | Frame overhead (unauthenticated encryption) | Counter length (in bytes) | Variable replay window (size) | Replay protection | Authentication length (bytes) | Integrity protection (algorithm) | Frame Encryption (Bulk - P2P only) | Native Ethernet Encryption | Encryption Modes | | Latency MP Mode cut-through | Lateriky FZF Midde Gut-fillodgin store & forward | Latanan DOD Mada ant theory | Latency | CFC | ASIC | FPGA | Encryption Hardware | store&tonward | cut-through | Processing Method | Key Length (in bit) | Alternative Mode of Operation | Block Cipher | Encryption Standard | Data Flarie Erictyption Standard and Flocessing | |
|----------------------------|---|---------------------------|-------------------------------|-------------------------------|----------------------------------|-------------------------|------------------------------|----------------------|---------------------------------|----------------------------|--|--|---------------------------|---|----------------------------|-------------------------------------|-------------------------------|-------------------|-------------------------------|----------------------------------|-------------------------|-----------------------------|---|-------------------------|----------------------------|---|---|---------------------------|-------------------------------|-------------------|-------------------------------|----------------------------------|------------------------------------|----------------------------|------------------|-------|-----------------------------|---|-----------------------------|---------|-----|------|------|---------------------|---------------|-------------|-------------------|---------------------|-------------------------------|--------------|---------------------|---|---------|
| s.ne | N/A | 80 | 0-30s | 01/10 | GCM | unlimited | unlimited | 32 | ٢ | < | 18/26 | N/A | τ α | . • | . ۲ | ۲ | 0-30s | ۲, | 8/16 | GCM | 256 | unlimited | 1000 | | WA | 18/26 | NA | œ | C 0-30s | < | 8/16 | GCM | ۲ | | | <48µs | <42µs | <42µs | | | | | ۲ | | ۲, | ۲, | | 256 | GCM | AES | | | |
| < 00 | NVA | 80 | • 0-30s | 8/16 | GCM | unlimited | unlimited | 32 | ٢ | | 18/26 | NIA | α | . < | . < | ۲, | 0-30s | ۲, | 8/16 | GCM | 256 | unlimited | 1000 | ÷ | WA | 18/26 | NA | œ | • 0-30s | • | 8/16 | GCM | ۲ | | | <48µs | -42µs | <4 <i>4</i> µs | | | | | ۲ | | ۲, | ۲ | | 256 | GCM | AES | | | |
| < . | N/A | 8 | 0-30s | 8/16 | GCM | unlimited | unlimited | 32 | ٢ | • | 18/26 | N/A | τ | . • | . ۲ | ۲, | 🗸 0-30s | ۲, | 8/16 | GCM | unlimited | unlimited | 1000 | | N/A | 18/26 | N/A | 00 | ✓ 0-30s | ۲ | 8/16 | GCM | ۲ | | | <9µs | <8µs | Srf6> | 0 | | | | ۲ | | ۲ | ۲ | | 256 | GCM | AES | | | Secunet |
| < s | N/A | 80 | < 0-30s | 01.0 | GCM | unlimited | unlimited | 32 | ۲ | < | 18/26 | NIA | р ч | . < | . < | ۲ | 🗸 0-30s | ۲ | 8/16 | GCM | 256 | unlimited | 1000 | | WA | 18/26 | N/A | - 00 | ✓ 0-30s | ٩ | 8/16 | GCM | ۲ | | | <4µs | <4µs | <4µs | -4100 | | | | ۲ | | ۲, | ۲ | | 256 | GCM | AES | | | Inet |
| < | N/A | 8 | < 0-30s | 8/16 | GCM | unlimited | unlimited | 32 | ۲ | • | 18/26 | N/A | τ | . • | ۰ ۲ | ۲ | 0-30s | ۲, | 8/16 | GCM | unlimited | unlimited | 1000 | | N/A | 18/26 | N/A | 00 | • 0-30s | ٦ | 8/16 | GCM | ۲ | | | <4µs | <4µs | <4µs | -4 | | | | ۲ | | ۲ | ۲ | | 256 | GCM | AES | | | |
| | | 8 | < 0-30s | 8/16 | GCM | unlimited | unlimited | 32 | ۲ | < . | 18/26 | N/A | α | . < | . < | ۲, | 🗸 0-30s | ۲ | 8/16 | GCM | 256 | unlimited | 1000 | | N/A | 18/26 | N/A | 00 | ✓ 0-30s | ۲ | 8/16 | GCM | ۶ | | | <2µs | <2µs | <2418 | -Oue | | | | ۲ | | ۲ | ۶ | | 256 | GCM | AES | | | |
| UL=XIMI. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Secunet

X=100%

| Traffic Flow Security | Based on VLANID and presence of MPLS tag MPLS EoIP IP Traffic Masking | Based on presence of MPLS tag MPLS EoIP IP | Based on VLANID MPLS EoIP IP | Combination of multiple selection oriteria Mixed Ethernet, MPLS, EoIP and IP Support | Based on MAC Address Based on VLAVID Based on Twitter Based on Multicast Group Based on Presence of WPLS Tag Based on Presence of WPLS Tag | Selective Encryption | Variable pipay window (size) Counter length (in bytes) Packet overhead authenticated encryption (AE) | Accultorial Autometricated Data (neader) | Integrity protection (algorithm) Authentication length (bytes) | Mxmum number of peers Maximum number of IP addresses Maximum number of multicast groups | Transport Tunnel Mode | TCP UDP | IPv6 Supported transmission protocols | Supported IP versions IPv4 | Native IP Encryption | Ethernet multi-hop support | Frame overhead unauthenticated encryption | Registered Ethertype Counter length (in bytes) | Replay protection Variable replay window (size) | Integrity protection (algorithm) Authentication length (bytes) | Max, number of VLAN IDs | Tunnel (Ethernet over IP) Supported transmission protocols (UDP/TCP) Max: number of peers Max: number of MAC Androsese | Ethernet over IP (EoIP) |
|--|---|---|---------------------------------------|---|---|----------------------|--|--|---|---|-----------------------|------------|--|-------------------------------|----------------------|----------------------------|---|---|--|---|-------------------------|---|-------------------------|
| • TFS mode only secure based on ASIC or FPGA | | , , , | , , , | < < | | | ♥ 0-30s 8 IPv4: 38/46, IPv6: 58/66 | | GCM | unlimited unlimited | 1 | ۰ ۲ | , | ۲ | | < - | N/A | ∞ ₹ | ९ 0-30s | GCM 8/16 | unlimited | native IP/UDP 2 (P2P), 1000 (MP) | |
| on ASIC or FPGA | ,,,, | ,,,, | * * * | ~ 7 | | | ♥ 0-30s 8 IPv4: 38/46, IPv6: 58/66 | < < | GCM 8/16 | unlimited unlimited unlimited | - | , , | , | ٢ | | • | N/A | ∞ ₹ | ९ ९ 0-30s | GCM 8/16 | unlimited | native IP/UDP 2 (P2P), 1000 (MP) | |
| ۲. | ,,,, | ,,,, | , , , | | | | V 0-30s 8 IPv4: 38/46, IPv6: 58/66 | < < | GCM 8/16 | unlimited unlimited unlimited | | , , | , | ٢ | | < . | N/A | œ र् | < 0.30s | GCM 8/16 | unlimited | native IP/UDP 2 (P2P), 1000 (MP) | |
| ۲ | | | , , , | | | | V 0-30s 8 IPv4: 38/46, IPv6: 58/66 | | GCM 8/16 | unlimited unlimited unlimited | 5 2 | , , | , | ٢ | | < - | N/A | œ ९ | ९ ९ ९ | GCM 8/16 | unlimited | native IP/UDP 2 (P2P), 1000 (MP) | |
| ۲ | | , , , | , , , | | | | ♥ 0-30s 8 IPv4: 38/46, IPv6: 58/66 | | GCM 8/16 | unlimited unlimited unlimited | - | , , | , | ٢ | | < . | N/A | co < | ९ ९ 0-30s | GCM 8/16 | unlimited | native IP/UDP 2 (P2P), 1000 (MP) | |
| ٩. | | | | | | | ✔ 0-30s 8 IPv4: 38/46, IPv6: 58/66 | | GCM | unlimited unlimited | - | 、、 | ۲, | ٢ | | • | N/A | ∞ < | ९ 0-30s | GCM 8/16 | unlimited | native IP/UDP 2 (P2P), 1000 (MP) | |
| _ | | | | | | | | | | | | | | | | | *11/17_100% | | | | | | |

| Session Key (UEK) Exchange Protocol Automatic Change of Session Keys Minimum Time Interval for Session Key Change (min) | Master Key (KEK) Agreement Master Key (KEK) Exchange Protocol Automatic Change of Maeter Key Minimum suggested Time Interval for Master Key Change (min) Separate Master Key (KEK) per site Separate Master Key (KEK) per goup Separate Master Key (KEK) per goup | Key Agreement and Key Exchange | Ad-hoc authentication of peers (manual) Signature key protocol | Asymmetric Signature: Certificate Maximum number of certificates per encryptor Key lenght | Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encryptor Key length | Device Authentication | CBC-MAC-GCM Key length | SHA-2 Key length | Hash Algorithms | Supported Curves: NIST Beatripool Gustom Curves | Elliptic Curve Cryptography (ECC) Key length | RSA Key length | Asymmetric Key Algorithms (Public Key Cryptography) | Hardware Random Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) | Key Generation and Storage | Key Management | Autonomous operation | Integrated Key Server Support for external Key Server External Key Server Support for multiple distributed Key Servers Support for rail-over to back-up Key Server | Key Server | Auto-discovery of network encryptors Auto-discovery of Key servers Auto-discovery of VLANs Disabiling of auto-discovery | Auto-discovery |
|---|---|--------------------------------|---|---|---|-----------------------|------------------------|------------------|-----------------|--|---|----------------|---|---|----------------------------|----------------|----------------------|--|------------|--|----------------|
| atmedia 1 | atmedia | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | | | | ۲ | ,, ,, | | ,,,, | |
| atmedia | ercKAS-DH***** | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | , , , | 512/521 | N/A | | телтр | | | ۲ | ,, ,, | | ,,,, | |
| atmedia | ecKAS.DH**** atmedia | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | , , , | 512/521 | N/A | | телтр | | | ٢ | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | | ,,,, | Se |
| -1 Califa | ECKAS-DH | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | TETP | | | ٩ | ,, ,, | | ,,,, | Secunet |
| - < | eCKAS-DH | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | телтр | | | ٩ | ,, ,, | | ,,,, | |
| atmedia | eCKAS-DH**** | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | \$12 (recommended:18) 256 | | 256 | 512 | | | 512/521 | N/A | | TETP | | | ۲ | 、、、、 | | 、、、、 | |

ECDSA optional for use with optional certificates ***NIST, Brainpool or custom curves with 256 to 521 bit length

| Group Key Distribution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAN ID Frames with MPLS tag IP Address IP Multicast Group | Group Membership Definition Multicast group membership Individual membership Network membership ULAN membership Trunked VLAN membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multicast.group Individual key per broadcast.group (VLAN ID) | Key assignment based on: MAC address (pairwise and mixed) Multicast groups (mixed) VLAN ID (group) Pon Group (group) IP Address IP Multicast Group | Multipoint Key System Supported key systems: Pairwise Group Mixed (pairwise unicast, group multicast) | Key assignment based on: NAC Address VLAN ID Pon Group IP Address | Point-to-Multipoint Key System Supported key systems: Pairwise Group | Key assignment based on: NLAN ID Pon Group IP Address | Key System Point-to-Point Key System Supported key system Pairwise Group |
|---|--|--|--|--|---|---|--|---|---|--|
| 、、 | * * * * * | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ~ | | ***** | Bidirectional Group | | Bidirectional Group | * * * * * | Bidrectional Group |
| | | * * * * * * | ۲. | • • | * * * * * * * | Bidirectional Group | * * * * * | Sidirectional Group | | Bidirectional Group |
| , , | ,,,,, | ***** | ~ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Sidirectional Group | ,,,,, | Sidirectional Group | ,,,,, | Bidriectional Group |
| | ,,,,, | ***** | ۲, | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | S Bidirectional Group | * * * * * | Sidirectional Group | ,,,,, | Belired onal Group |
| , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | * * * * * * | 2 | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Sidirectional Group | * * * * * | € Bidirectional Group | ,,,,, | Bdirectional Group |
| | ,,,,, | | ۲ | 、 、 | ***** | Bidirectional Group | ,,,,, | Sidirectional Group | , , , , , | Bidirectional Group |

| Boot Time Cold boot until operational Warm boot until operational | Security Approvals Safety Approvals | Height in 19" Rack Number of external encrypted Ethemet ports Physical Device Access Redundant Power Supply Redundant, hot-swappable power supply Heigh Availability functionality (two-node cluster) High Availability functionality (two-node cluster) MTBF Tamper Security | Sysiag Support (Server) | Logs Event Log (local) | In-band Management SSH SNMP (read-only/read-write) TLS Proprietary Remote Monitoring (SNMP) | IPv4 IPv6 Out-of-band Management RS-232/V.24 Separate Ethemet port Smart Card (Secure Card) Support USB Port | Munipoint Dead Peer Detection Optical Loss Pass-Through Link Loss Carry Forward System Configuration and Management Access | Network Support Europ in the Wire deployment Jumbo Frame Support Ethernet Flow Control via PAUSE Ethernet FragmentationDefragmentation Point-to-Point Point-to-Multipoint Multipoint |
|---|---|---|-------------------------|---------------------------|--|--|--|---|
| 256 278 | | 1U 1 back 1:1 50.000h TE/TP | ς, | | read-only v2cv3 | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | (2 () | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |
| 25s 25s 25s 27s 27s 27s | BSI VS-NfD, NATO restri EN55032 Clas | ۱۵ ۲:1 ۲:1 ۲:1 ۲:2000h | ۰ ، | | read-only v2c/v3 | **** | ۲ <u>۸</u> ۲ | |
| 25s 27s | BSI VS-NID, NATO restricted, EU Restrint (including 2nd Evaluation by NL) EN55022 Class B, FCC Part 15 Class B, ROHS | 1U 1 50000h TE/TP | 、 、 | | read-only v2cv3 | **** | | |
| 25s 27s | l Evaluation by NL) IS | 1∪ 1 € € 50000h | < · | | vac t | **** | | |
| 25s 27s | ***** | 10 14 14 1:1 1:1 1:1 1:1 1:1 1:1 | | | read only v2ov3 | * | Z (() | |
| 25s 27s | ***** | 10 1-4 1-1 1:1 7E/TP | ς, | | read-only v2c/v3 | **** | \$ | |

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

| Warranty Period (months) Warranty Coverage Parts & Work Basic Support (9 to 5, e-mail, phone) Software updates and upgrades Warranty Extension (per year) | List Price Encryption Unit (in €) Per external Key Server (in €); optional, no requirement Required Management Software (SINA Software optional) 2-10 encryptors 11-25 encryptors 26-50 encryptors 51+ encryptors | Certificate Creation Certificate Management Group creation Group isolation Key assignment Fail-over configuration | Role-based access Identity-based authentication of user Number of hierarchy levels Strict internal separation of users Device Management Device Diagnostics Link Montoring (SNMP) Connecton Diagnostics In-band Matwork Diagnostics Remote Update/Upgrade Centificate Authority & Management | User Interface Native PC application Embedded Wetapp CL Initial Device Set-up Device Configuration Local (out-of-band) Remote (out-of-band) Remote (in-band) Remote (in-band) Device Configuration Local (out-of-band) Remote (in-band) | Management Software |
|---|---|--|--|--|---------------------|
| on valuest | on request included included included included | optional states | ορίσηαι | | |
| on request | on request included included included | cccc optional | ορίση | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | |
| on request | on request on request included included included | ç t t t t t optional | | ,,, ,, ,, , | |
| on request | on request on request included included included | optional | optional | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | |
| on request | on request on request included included included | optional CCCCC | ορίο | , | |
| on request | on request on request included included included | optional optional | ορθοη <u>αι</u> | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | |

gga

| S |
|----------|
| Ō |
| C |
| _ |
| 3 |
| ŏ |
| ÷. |
| ŵ. |
| |

| Platform Platform used Mainboard/Firmware Key Management | Single tenant Single tenant Multi-tenant Self-managed Managed encryption service Managed security service | Supported Networks (Transport of Encrypted Frame) Ethemet (native) MPLS (EoMPLS) IPv4/IPv6 TCP UDP | Supported Networks (Encryption) Ethemet MPLS IP v4/v6 | Port-based Ethernet Private Line (EP-Line) Ethernet Private Lane (EP-Line) Ethernet Private LAN (EP-LAN) VLAN-based Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private LAN (EVP-LAN) | Point-to-Point (P2P) Point-to-Multipoint (P2MP) Multipoint (MP) Supported Metro Ethernet Topologies | Line Interface/Supported Line Rates 10 Mbs 100 Mps 10 Gbps 25 Gps 40 Gbps 100 Gbps 100 Gbps 100 Gbps 100 Gbps 100 Gbps 100 Gbps 100 Gbps 100 Gbps 100 Gbps |
|---|--|--|--|---|--|--|
| almedia/almedia almedia | | * * * * * | | | | Centurion 50/100 compact V.R.445 V.R.45 V.R.45 |
| atmedia/atmedia atmedia | * * * * * | * * * * * | * * * | | * * * | Centurion 50/100 compact |
| atmedia/atmedia atmedia | * * * * * | * * * * * | | | • • • | V.R.45 V.R.45 V.R.45 V.R.45 |
| atmedia/atmedia atmedia | | * * * * * | , , , | | , , , | Centurion 16 V/SFP V/SFP V/SFP |
| atmedia/atmedia atmedia | | * * * * * | , , , | | , , , | Centurion 10G V/SFP+ V/SFP+ V/SFP+ |
| atmedia/atmedia atmedia | | * * * * * | | | | Centurion 40G VOSEP VOSEP VOSEP VOSEP |
| almedia almedia | | * * * * * | | | | Centurion 100G Roadmap 04 2017 VIOSFP28 VIOSFP28 VIOSFP28 |

| Tunnel (Elhernet) Max. number of peets Max. number of MAC Addresses Max. number of VLAN IDs Integry protection (abgrithm) Authentication length (bytes) Replay protection Variable replay window (size) Counter length (in bytes) Frame overhead unimenticated encryption Frame overhead unimenticated encryption (AE) Ethernet multi-hop support | Transport (Psyload only) Max. number of VAC. Addresses Max. number of MAC. Addresses Max. number of VLAN IDs Inegrity protection (abjorithm) Authentication (abjorithm) Variable encryption offset (fixed) Definable encryption offset (fixed) Adaptive encryption offset (fixed) Counter keight (in bytes) Frame overhead authenticated encryption only Frame overhead authenticated encryption (AE) Ethernet multi-hop support | Encryption Modes Native Ethernet Encryption Fame Encryption (guik - R2 only) Integrity protection (elgorithm) Replay protection (elgorithm) Counter length (in bytes) Fame overhead (unathenticated encryption) Fame overhead (unathenticated encryption) Ethernet multi-hop support | Encryption Hardware FPGA ASIC CPU Latency Latency MP Mode cul-through Latency MP Mode cul-through store & forward | Processing Method cut-through store&forward | Data Plane Encryption Standard and Processing Encryption Standard Book Opher Preferred Mode of Operation Alternative Mode of Operation Key Length (in bit) | |
|--|--|--|--|---|---|-----------|
| Solver | uniimia 256 8/60 8/7 8/7 8/7 8/7 8/7 8/7 8/7 8/7 8/7 8/7 | NA NA | <42,15 <42,15 <42,15 <42,15 | 、、 | AES GCM 256 | |
| C 2028 C 2028 | unlimited unlimited B/CM 8/CM 8/CM 8/CM 8/CM 8/CM 8/CM 8/CM 8 | С С 8/16 8/16 8/18 8/18 8/18 8/18 8/18 8/18 | <abr></abr> equals | ~ ~ | AES GCM 256 | |
| unlimited 92 € 9308 9308 9308 8 9308 9 9388 9 9388 9 9388 9 9388 9 9388 9 9388 9 9388 9 9388 9 9388 9 9388 9 9388 9 938 9 938 9 938 9 938 9 938 9 938 9 938 9 938 9 938 9 938 9 938 9 938 9 9 9 9 | unlimbed 2.56 8.70 18.26 N.N.8 8.7 18.26 | N/A 18/26 N/A 18/26 | <42/1s <42/1s <42/1s | ~ ~ | AES GCM 256 | |
| 32 uniimited SCM 8/16 8/16 8/16 8/16 0-305 8/16 0-305 8/16 0-305 8/16 0-305 8/16 0-305 8/16 0-305 8/16 0-305 8/16 0-305 10 10 10 10 10 10 10 10 10 10 10 10 10 | ₹ 8 /10 1 /10 | СС СС 8 6 8 76 8 76 8 76 8 76 8 76 8 76 8 76 | ත්ර ක්රී ක්රී | , , | AES GCM 236 | Securosys |
| 32 untimited GCM 8/6 8/6 8/30s 8/0/30s 8/0/30s 8/0/30s 8/0/30s | unfinited 256 8/16 8/18 8/18 8/18 8/18 8/18 8/18 8/1 | NA 8 8 1828 8 1826 8 18 18 18 18 18 18 18 18 18 18 18 18 1 | stb> دراج> دراجه دراجه | ~ ~ | AES GCM 256 | |
| 32 GCM SCM SCM SCM SCM SCA SCA SCA SCA SCA SCA SCA SCA SCA SCA | vnimted 8/6 8/7 8/26 8/7 8/26 | NN A 8 8 16 16 16 16 16 16 16 16 16 16 16 16 16 | 5455 5475 5475 5475 5475 | ~ ~ | AES GCM 258 | |
| uniimited GCM 8 6 8 7 6 8 7 6 8 7 6 8 7 6 8 7 6 8 7 6 8 7 6 8 7 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 | uniimia 256 876 876 876 876 876 876 876 876 876 87 | С С 816 826 826 826 826 826 826 826 826 826 82 | 41/5 41/5 41/5 41/5 | ~ ~ | AES GCM 256 | |

*IMIX=100%

| Traffic Masking Traffic Flow Security | Based on VLAN ID and presence of MPLS tag MPLS EoIP IP | Based on presence of MPLS tag MPLS EoIP IP | Based on VLAN ID MPLS EoIP IP | Mixed Ethernet, MPLS, EoIP and IP Support | Based on MAC Address Based on VLAN ID Based on Fuerpo Based on Multicast Group Based on Presence of MPL/S Tag Based on Presence of MPL/S Tag Based on Presence of MPL/S Tag | Selective Encryption | Transport Tunnel Mode Maximum number of peers Maximum number of IP addresses Integrity protection (algorithm) Authentication length (foltes) Additional Authenticated Data (feader) Regar Protection Variable replay window (size) Counter length (in bytes) Packet overhead authenticated encryption (AE) | Supported IP versions IPv4 Supported transmission protocols TCP UDP | Native IP Encryption | Tunnel (Ethernet over IP) Max. number of peers Max. number of PACA Addresses Max. number of VAN IDs Integrity protection (algorithm) Authentication length (tyrtes) Authentication length (tyrtes) Authentication length (tyrtes) Authenticated data) Regizery protection Regizery protection Statistic replay window (size) Regizer of the type Counter length (in thytes) Frame overhead authenticated encryption Frame overhead authenticated encryption Ethernet mult-hop support | Ethernet over IP (EoIP) |
|---|---|---|--|---|---|----------------------|---|---|----------------------|---|-------------------------|
| ۲. | 、、、 | | | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | | unlimited unlimited GCM 8/6 9 0-30s 8 8 8 8 | ,, ,, | | 2 (PSP), i coo (MP) 2 (PSP), i coo (MP) unimited GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | |
| ۲ | ,,, | , , , | , , , | | ,,,,,,,,,,, | | uniimted uniimted GCM 8/16 • • • • • • • • • • • • • • • • • • • | ,, ,, | | 2 (P2P), 1000 (MP) 2 (P2P), 1000 (MP) unimited GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | |
| ۲ | | | ,,, | | ***** | | unlimited unlimited GCM 876 0.30s 8 8 1Pv4: 3846, IPv6: 5866 | ,, ,, | | 2 (P2P), 10/UDP unlimited GCM GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | |
| ۲ | , , , | , , , | ,,, | | ***** | | unlimited unlimited GCM 876 876 0-308 8 8 1Pv4: 3846, IPv6: 5866 | ,, ,, | | native PUDP 2 (P2P), 1000UP unlimited GCM 8/16 8/462 54/82 | |
| ٢ | ,,, | , , , | ,,, | | * * * * * * * * * | | unlimited unlimited GCM 8/16 0-308 8 1Pv4: 3846, IPv6: 5866 | ,, ,, | | 2 (P2P), 1000 (MP) 2 (P2P), 1000 (MP) unlimited GCM 6,716 8/16 8/16 8/16 5/162 | |
| ۲ | | , , , | ,,, | | * * * * * * * * * | | unlimited unlimited GCM 8/16 0-308 8 1Pv4: 38/46, 1Pv6: 58/66 | ,, ,, | | 2 (P2P), 1000 (MP) unlimited GCM 6 0 308 7 0 308 8 16 8 16 8 16 8 16 8 16 8 16 8 16 8 1 | |
| s, | ,,,, | 、、、 | , , , | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | | unlimited unlimited GCM 8/16 0-30s 8 IPv4: 38/46, IPv6: 58/66 | ,, ,, | | 2 (P2P), to (PUDP unimited unimited GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | |
| *TFS mode only secure based on ASIC or FPGA | | | | | | | | | | -IMX~100% | |

Securosys

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

***ECDSA optional for use with optional certificates

Automatic Change of Session Keys Minimum Time Interval for Session Key Change (min)

| Group Key Distribution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAN ID Frams with MPLS tag IP Address IP Muticast Group | Group Membership Definition Multicast group membership Individual membership Network membership VLAN membership Trunked VLAN membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multicast group Individual key per broadcast group (VLAN ID) | Key assignment based on: MAC address (pairwise and mixed) Multicast groups (mixed) VLAN ID (group) Port Group (group) IP Address IP Multicast Group | Multipoint Key System Supported key systems: Pairwise Group Mixed (pairwise unicast, group multcast) | Key assignment based on: MAC Address VLAN ID Port Group IP Address | Poin-to-Multipoint Key System Supported key systems: Pairwise Group | Key assignment based on: NAC Address LAN ID Port Group IP Address | Key System Point-to-Point Key System Supported key system Pairwise Group |
|---|--|--|--|--|--|--|---|--|--|--|
| | ,,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ۲. | 、、 | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Bidirectional Group | ,,,,, | Bidirectional Group | ,,,,, | e Bidiredional Group |
| , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ,,,,,,, | ۲ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Ridirectional Group | , , , , , | K Bidirectional Group | * * * * * | K Bidirectional Group |
| , , | ,,,,, | ,,,,,,, | ۲ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ► Bidirectional Group | , , , , , | ► Bidirectional Group | * * * * * | K Bidirectional Group |
| , , | ,,,,, | , , , , , , , | ۲ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Ridirectional Group | , , , , , | K Bidirectional Group | * * * * * | K Bidirectional Group |
| ~ ~ | ,,,,, | | ۲ | * * | ***** | Ridirectional Group | 、、、、、 | K Bidirectional Group | * * * * * | √ Bidirectional Group |
| , , | ,,,,, | , , , , , , , | ۲ | , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ► Bidirectional Group | , , , , , | ► Bidirectional Group | * * * * * | K Bidirectional Group |
| | ,,,,, | * * * * * * | ۲. | | ***** | Bidirectional Group | ,,,,, | Skilrectional Group | * * * * * | Sidrectional Group |

Securosys

| Boot Time Cold boot until operational Warm boot until operational | Security Approvats Satety Approvats | Height in 19" Rack Number of external encrypted Ethemet ports Physical Device Access Redundant Power Supply Redundant, hot-swappable power supply High Availability functionality (two-node cluster) MTBF Tamper Security | Logs Event Log (local) Audit Log (local) Systog Support (Server) Unit | Network Support Bump in the Wire deployment Jumbo Frame Support Ethernet Fragmentation/Defragmentation Point-to-Point Optical Loss Pass-Through Dead Peer Detection Optical Loss Carry Forward System Configuration and Management Access IPv6 Out-of-band Management USB Pont Smart Card (Secure Card) Support USB Pont In-band Management Strat Card Secure Card) Support USB Pont In-band Management Strat Card Secure Card) Support USB Pont In-band Management Strat Card Secure Card) Support USB Pont In-band Management Horband Management Strat Strat Card Secure Card) Support USB Pont Strat Card Secure Card) Support USB Pont In-band Management Horband Management Strat Strat Card Secure Card) Support Hemote Monitoring (SNMP) |
|---|---|--|---|---|
| 25s 27s | | 1U 1 back 1:1 > 50,000h TE/TP | | |
| 25s 27s | ***** EN5503 | 1U 1 1:1 > 50000h TE/TP | | |
| 25s 27s | ***** EN55032 Class B, FCC Part 15 Class B, ROHS | 10 front 1:1 59.000h TE/TP | | |
| 25s 27s | B, ROHS | 1U front 1:1 50,000h TE/TP | | |
| 25s 27s | ***** | 10 1 front 1:1 750,000h TE/TP | , , , | |
| 25s 27s | ***** | יו ט א ליט גע דברדף | | |
| 25s 27s | ***** | 10 1-4 1-4 1-1 1:1 1:1 1:1 1E/TP | | |

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

| List Frice Encryption Unit (In €) Per external Key Server (In €) optional, no requirement Required Management Software 2-10 encryptors 8±50 encryptors 8±50 encryptors 51+ encryptors Warranty Period (months) Warranty Ceverage Parts & Work Basic Support (I lo 5, e-mail, phone) Software updates and upgrades Warranty Extension (per year) | Key Management Group creation Group isolation Key assignment Fall-over configuration | Device Management Device Diagnostics Link Monitoring (SNMP) Connection Diagnostics In-band Network Diagnostics Remote Update/Upgrade Certificate Authority & Management Certificate Creation Certificate Management | Management Access Role-based access Identity-based authentication of user Number of hierarchy levels Number of hierarchy levels Strict internal separation of users | Device Configuration Local (out-of-band) Remote (in-band) Remote (out-of-band) | Embedded Webapp CLI Initial Device Set-up Local (out-of-band) Remote (out-of-band) | Management Software User Interface Native PC application |
|--|--|---|--|---|--|---|
| on request included included included included included on request on request | | optional optional | ζωνζ | | 、、、、 | ۰. |
| on request included included included included on request on request on request | | optional | ζσΝζζ | | 、、、、 | ۲. |
| on request included included included included con request on request on request | | optional | S OT IN S S | | ,, , | ۲. |
| on request included included included included con request on request | | optional | S OT IN S S | | 、、、、 | ۲ |
| on request included included included included con request on request on request | , , , , | optional optional | S OT NO S S | ,,,, | , , , | 、 |
| on request included included included included on request on request on request | , , , , | optional optional | (07 N) ((| ,,,, | , , , | ۲. |
| on request included included included included con request on request on request | ,,,, | optional optional | S (J) N S | * * * | ,,,, | |

02007 - 2017 Christoph Jaggi ALL RIGHTS RESERVED

Securosys

| | Platform used Mainboard/Firmware Key Management | Platform | Self-managed Managed encryption service Managed security service | Single tenant Multi-tenant | IP will Pvd UDP UDP | Supported Networks (Transport of Encrypted Frame) Ethernet (native) | Ethernet MPLS (MPLSoE) IPv4/IPv6 | Supported Networks (Encryption) | VLAN-based Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private Tree (EVP-Tree) Ethernet Virtual Private LAN (EVP-LAN) | Portbased Ethernet Private Line (EP-Line) Ethernet Private Tree (EP-Tree) Ethernet Private LAN (EP-LAN) | Supported Metro Ethernet Topologies | Point (o-Point (P2P) Point to-Multipoint (P2MP) Multipoint (MP) | Supported Network Topologies | Virtual Appliance | 10 Mbs 100 Mps 1 Gbps 10 Gbps 25Gps 40 Gbps 100 Gbps | Line Interface/Supported Line Rates |
|---|--|----------|--|-------------------------------|---|--|--|---------------------------------|--|--|-------------------------------------|---|------------------------------|-------------------|--|-------------------------------------|
| * IP support only in combination | Senetas/Senetas Senetas | | , , , | ۲ ۰ ۲ | | ς ς | , , | | , , , | ,,, | | , , , | | | ▲ FRU45 ▲ FRU45 | CN4010 |
| * IP support only in combination with TBANSEC and limited to P2P. Additional overhead and latency | Senetas/Senetas Senetas | | | * < | | | , , | | | | | 、、、 | | | < SFP < SFP | CN4020 |
| P Additional overhead and later | Senetas/Senetas Senetas | | , , , | . ۲ | | ς ς | , , | | , , , | , , , , | | , , , | | | V.R.UAS/S.FP V.R.UAS/S.FP V.R.UAS/S.FP | CN6010 |
| 2 | Senetas/Senetas Senetas | | ,,,, | × < | | < < | | | 、、、 | | | , , , | | <u>c</u> | S SFP | CN6100 |
| | Senetas/IDQuantique Senetas | | | ✔ Vone tenant per port | | | | | | | | | | | V/SFP+ V/SFP+ V/SFP+ V/SFP+ V/SFP+ | CN8000 |
| | Senetas/Senetas Senetas | | | ۰ ۲ | • Roadmap Q4 2017 • Roadmap Q4 2017 • Roadmap Q4 2017 | | | | | | | | | | V/GFP-4 | CN9100 |
| | Senetas/Senetas Senetas | | | ¢ | * Roadmap Q4 2017 * Roadmap Q4 2017 * Roadmap Q4 2017 | | | | | | | • • • | | | V/OSFP-28 | CN9120 |

*1P 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

| Tund (Ethernet) Max. mithe of cheers Max. mathe of cheers Max. mathe of AVAC Address Max. mathe of AVAC Address Max. mathe of AVAC Dist Inappy protection Address protection Address protection Variable address protection Caratre weight in birden Famino ownerskal subanitizated excryption (AE) Ethernet math-top support | Tampon (Payload only) Mix. numbe of MAC A doteses Mix. numbe of MAC A doteses Mix. numbe of VLAL IDS Mix. numbe of | Native Ethernet Exception Frame Encryption (Built - P2P only) Imaging protection (apportun) Authentication (application) Regist protection Vanish encoders Control worth (in System) Frant overhead (authenticated encryption) Ethernet maticipe appoint | Lutency Latency P2P Mode celefrough Latency M2 Mode celefrough Latency M2 Mode celefrough Store & Korward Encryption Modes | Processing Method storactoreard Encryption Hardware ASC CPU | Onte Plane Encryption Standard and Processing Encryption Standard Book Oper Peternet Mode of Operation Any sequin (not Operation Key sequin (not Operation | |
|--|---|--|---|---|---|---------|
| 2 . unimmed unimmed GGM 16 244 fumme 245 fumme 2 | 4000 Unitemed 284 GGA 16 5 5 5 5 5 5 5 6 0 (CCTR) 24 0 (CCTR) | COM 16 256 Firms 5 5 8 (CTR) + Luneel (min 16 Exples) 24 + Luneel (min 19 Exples) | <10/3 (@10569) <10/3 (@10569) | ۲۰۰۶ | AES GCM CFBC/TH 128/256 | |
| 2 e uritimmed uritimmed GCM 16 CCM 265 emes 5 5 8 (CTM) 24 + turnel (min. 18 bytes) | 0 (CFB) 4 (CTR) 256 6 (CM) 256 6 (CM) 256 8 (CTR) 256 (CTR) 24 | GCM 16 26 fumes 5 (CTR) + strong (Trice 18 bytes) 24 + turnel (min 18 bytes) | <10/ж (@105ps) | x . x | AES GCB CEBCCIR 128256 | |
| 2 unimoted unimoted GCM GCM 255 tames 5 5 8 (CTR) 8 (CTR) 8 (CTR) 8 254 tames 254 tames 254 tames 8 (CTR) 8 (CTR) 10 10 10 10 10 10 10 10 10 10 10 10 10 | 40000/united 226 300 16 266 sames 266 sames 26 | eCM 16 256 turnes 5 8 (CTFR + turnel (min. 18 bytes) 24 + turnel (min. 18 bytes) | -10µ8 | ۲۰۰۶ | AES GCBUCTR 128/256 | |
| 2 unimoted unimoted GCM GCM B (CTR) B (CTR) B (CTR) B (CTR) B (CTR) C | 40000/united 512 600 16 26 \$annes 26 \$annes 26 \$annes 2 \$ \$ \$ 5 \$ 5 | eCM 16 26 turnes 5 8 (CTF) + turnel (min. 18 bytes) 24 + turnel (min. 18 bytes) | - & - \$s | ۲. ۲ | AES GCRA CFBCCTR 128/256 | Senetas |
| | 40000/unimed 5/12 6/0 16 256 frames 256 frames 256 frames 256 frames 26 frames 26 frames 26 frames 2 f | | · ర్ష ర్షి | ۶۰۰۶ | AES GCDR CFBCCTR 128/256 | |
| . Реалтар О4 2017 | 512 40000/utimined 512 COM (Readiming O4 2017) 16 256 frames 5 5 5 6 5 5 8 (5 TFI) 2.2 | * Readmap 04 2017 | stro Sta | | AES GCM (Roadmap 04 2017) 128256 | |
| - Roadmap 64 2017 | 512 4000/unimed 512 206 Rumes 5 206 Rumes 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | "Roatmap Of 2017 | ette Atte | | AES CTR GCM (Readmap C4 2017) 128/256 | |
| | limitation only in MAC mode | | | | | |

| Based on VLAN 10 and presence of MPLS tag MPLS Ecolo IP | Based on presence of MPLS tag MPLS EoIP IP | Baad on VLAN D Baad on VLAN D MPLS Eolp | Baad on WAC Address Baad on Ennryse Baad on Ennryse Baad on Makous Group Baad on Pawaros ot Ma S Tag Baad on IP Adgress Baad on IP Adgress Combination dimultiple selection criteria | Transport/mend Mode Mommunute of pears Maximum number of Padresses Controls Water Sector Number Sector Number of Padresses Sector Number of Padresses | Supported IP venions IP-4 Supported Transmission protocols UDP | Native IP Encryption | Tumol (Energed over IP) Supposed transition proceeds (UDP/TCP) Max. number of MAXC Addresses Counter & Hugh (n Maxed) Finite overhead a matericable acception (AE) Enservice intrology anged Enservice intrology anged | Ethernet over IP (EoIP) |
|--|---|--|---|--|---|----------------------|--|-------------------------|
| | | | | | | | U0) uni 0 259 8 (CTR) + turn 8 (CTR) + turn 8 (CTR) + turn | |

Traffic Masking Traffic Flow Security

map Q4 2017

p Q4 2017

| x | 、 、、、、 | | UpPrtp 2 untimeted CCM 2 2 for united 2 for |
|-----|--------|--|---|
| ×. | , ,,,, | | UDPTCP 2 unimeted unimeted unimeted 0 CR 2 8 (CTFR) + June 8 (CTFR) + June 8 (CTFR) + June 8 (CTFR) + June 8 (CTFR) + June 8 (CTFR) + June 8 (CTFR) - Style 2 (CTFR) - Style 2 (|
| ς. | | | UDPTCP 2 unimoted uni |
| s. | , ,,,, | | UDPT CP 2 unimoted unimoted unimoted unimoted UCM 4 4 8 6 7 1 8 6 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 |
| ¢. | , ,,,, | | |
| < c | , ,,,, | | • Reading 04 2017 |
| | | | • Feating Od 2017 |

| æ |
|---|
| - |
| Ð |
| a |
| s |
| |

| Susion Key (DEK) Eichnage Argement Susion Key (DEK) Eichnage Probod Aubrate Key (DEK) Eichnage Vrober Aubrate Key (DEK) Eichnage (min) Meimum Time Interval for Susion Key Charge (min) | Master Koy (KEK) Agement Master Koy (KEK) Exchange Protocol Automate Change of Master Koy Minimum suggested Time Interval for Master Key Change (min) Separate Master Koy (KEK) per group Separate Master Key (KEK) per group | Key Agreement and Key Exchange | Ad-hoc authentication of peers (manual) Signature key protocol | Asymmetric Signature: Certificate Maximum number of certificates per encryptor Key (ength | Symmetric Signature: Preshared Key (PSK) Maximum number of PSKs per encryptor Kay length | Device Authentication | SHA-2 Key length | Hash Algorithms | Supported Curves: NIST Brähpod Custom Curves | Key length | Elliptic Curve Cryptography (ECC) | RSA Keylength | Asymmetric Key Algorithms (Public Key Cryptography) | Hardware Random Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) | Key Generation and Storage | Key Management | Autonomous operation | Ining stadi Kry Server Support for selamal Kry Sanet Estenati Kry Server Support for Ital-orier to back-up Kry Server Support for Ital-orier to back-up Kry Server | Key Server | Auto-discovery of network encryptors Auto-discovery of two servers Auto-discovery of VLANs Disabiling of auto-discovery | Auto-discovery |
|--|--|--------------------------------|---|---|--|-----------------------|------------------|-----------------|---|------------|-----------------------------------|---------------|---|---|----------------------------|----------------|----------------------|--|------------|--|----------------|
| | | | _ | | | | _ | 1 | _ | | | | 1 | _ | | _ | ļ | _ | _ | | _ |
| 1TM Forum Security Specifications NIST SP800-56A | ECDH/RSA Senetas 1440 | | ECDSARSA | x 509 64 512 (ECC)/2048 (RSA) | | | 512 | | , , , | 512 | | 2048 | | د TE/TP | | | ۲ | ,, ,, | | | |
| ATM Forum Security Specification NIST SP800-56A | ECDH/RSA Serretas 1440 | | ECDS A/RSA | x 509 64 512 (ECC)/2048 (RSA) | | | 512 | | ,,, | 512 | | 2048 | | TE/TP | | | ۲ | ,, ,, | | * * * * | |
| s ATM Forum Security Specification NIST SP800-56A | ECDH/RSA Senetas 1440 | | ECDSWRSA | x. 509 64 512 (ECC)/2048 (RSA) | | | 512 | | | 512 | | 2048 | | TE/TP | | | ۲ | 、、、、 | | | |
| s ATM Forum Security Specifications NIST SP800-56A • | ECDH/RSA Senretas 1440 | | ECDSA/RSA | x.509 64 512 (ECC)/2048 (RSA) | | | 512 | | ,,, | 512 | | 2048 | | телр | | | ۲ | ,, ,, | | ,,,, | Senetas |
| ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Senetas 1440 | | ECDSA/RSA | x.509 64 512 (ECC)/2048 (RSA) | | | 512 | | ,,, | 512 | | 2048 | | ✔/ORNG TE/TP | | | ۰ | ,, ,, | | ,,,, | |
| ATM Found Security Specifications ATM Fo | ECDH/RSA Senetas | | ECDS A/RSA | x.509 64 512 (ECC)/2048 (RSA) | | | 512 | | ,,, | 512 | | 2048 | | ✔ QRNG TETP | | | ۲ | ,, ,, | | ,,,, | |
| ATM Forum Security Specifications NIST SP800-56A | ECDH/RSA Serretas 1440 | | ECDSA/RSA | x.509 64 512 (ECC)/2048 (RSA) | | | 512 | | ,,, | 512 | | 2048 | | ✓/QRNG TE/TP | | | ٢ | <i>、、、、</i> | | ,,,, | |

| Group Key Distribution Unicast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC activess VLAN ID Frames with MPLS tag IP Actives IP Muticast Group | Group Membership Definition Muticast group membership Individual membership VLAW membership Trunked LAM membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multcast group Individual key per broadcast group (VLAN ID) | Key assignment based on: Multi-ast groups (mixed) VLAN ID (group) Port Group (group) IP Address IP Multi-ast Group | Multipoint Key System Supported key systems: Patrivee Group Mixed (patrivise unicast, group multicast) | Key assignment based on: MAC Address ULAN ID Port Group IP Address | Point-to-Multipoint Key System Supported key systems: Painvise Group | Key assignment based on: MAC Address VLAN ID Port Group IP Address | Point-to-Point Key System Supported key system Patrivise Group | Key System |
|---|---|--|--|---|--|--|---|---|---|---|------------|
| 、、 | , , | | ۲. | • • | **** | Bidirectional Group | ,,,, | Sectional Group | ,,,, | Bidirectional Group | |
| ~ ~ | , , | *** * | ς. | • • | **** | Bidirectional Group | **** | Skirectional Group | **** | Bklirectional Group | |
| , , | , , | , , , , | ۶ | , , | ,,,,, | Bidirectional Group | ,,,, | ► Bidirectional Group | | Sidirectional Group | |
| ~ ~ | | *** * | ۲ | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | Sidirectional Group | * * * * | Sidirectional Group | ,,,, | Bidirectional Group | Senetas |
| | | *** * | <. | • • | ,,,,, | Sidirectional Group | ,,,, | Sidirectional Group | **** | Bidirectional Group | |
| ~ ~ | , , | | ۲. | • • | ,,,,, | Bidirectional Group | ,,,, | S Bidirectional Group | * * * * | Bidirectional Group | |
| | | | ۲. | | **** | Bidirectional Group | **** | Sidirectional Group | **** | Bidirectional Group | |

| Cold boot until operational (P2P) Warm boot until operational (P2P) | Boot Time | Security Approvals Safety Approvals | Height in 19° Rack Number of external encrypted Ethernet ponts Phyrael Devic Acoss Redundant Rover Skepty Redundant Rover skepty High Availability functionality (their node cluater) MTBP Tamper Security | Logs Event.og (oca) Add.fog (oca) Saylog Seport (Sarver) Unit | In-band Management SHM (read-only/nad-write) TLS Proposity Remote Montoing (SM/P) | IPA IPA Out-d-band Managament B3-2207.24 Spanar Card (Secure Card) Support USB Port | Link Loss Cany Forward System Configuration and Management Access | Burp in the Wei degoyment Unito Ferrers Suport Ehemet Fow Control via PAUSE Ehemet Fragmentation Del systemation Point-ce-Nuthoot Matipoint Dead Peer Detection Dead Peer Detection | Network Support |
|--|-----------|--|---|---|--|--|--|--|-----------------|
| 65s 80s | | FIPS 140-2 L3, CC EAL2+, UC APL, NATO EN55022 class B, EN61000, ROHS | Desktop t back Readings 2017 >200.000h TE/TP | | RORW V1/A22V3 | < <<< << | <. | , ,, | |
| 65s 80s | | FIPS140-2 L3, CC EAL2+, UC APL, NATO EN55022 class B, EN61000, ROHS | DaveKop back Roadmap 2017 > 200.000h TE/TP | | ROURW VI AZENS | | . | , , , , , , , , , , , , , , , , , , , | |
| 65s 80s | | FIPS140213, CC EA124, UC APL, MITO FIPS140213, CC EA124, CC E | 1U 1 front € Roadmap 2017 > 20000th 7E/TP | ,,, | ROAW V1/AZOV3 | , , , , , | . | | |
| 65s 80s | | FIPS140-2 L3, CC EAL2+, UC APL, NATO EN55022 class B, EN61000, ROHS | rtu 1 Nonti Roadmap 2017 > 200 00/h TE/TP | | RORW V1/22A3 | < < < < < | ج ۱ | | |
| 65s 80s | | FIPS140-2 L3, CC EAL2+ EN55022 dass B, EN61000 ROHS | 4U 1-10 front Nondmap.2017 >100.000h TE/TP | | ROAW V1/V2cM3 | < < < < < | ۲. | | |
| 65s 80s | | FIPS140-2 L3/CC EAL2+ in progress EN55022 class B, EN61000, ROHS | 1U 1 Front € Readmap 2017 > 200 00th TE/TP | | RORW V1/N2EW3 | < < < < < | ۲. | | |
| 65s 80s | | EN55022 class B, EN61000, ROHS | 1U - Foot € € Foodmap 2017 > 200000h TE/TP | | RORW | < < < < < | ح ۱ | | |
| | | CC EAL2+, FIPS 140-2 L3, UC APL/CPA in progress/planned | | | | | | | |

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

| 9 0 | |
|---|--|
| | |
| | |
| | |
| | |
| 5 | |
| Į. | |
| Š. | |
| | |
| 3 | |
| 8 | |
| | |
| | |
| | |
| | |
| | |
| ť. | |
| 7 | |
| P | |
| 0 | |
| ij | |
| | |
| | |
| | |
| | |
| | |
| hen | |
| | |
| 5 | |
| 5 | |
| 5 | |
| ē | |
| | |
| | |
| 2 | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| or file m | |
| | |
| or file m | |
| or file modificat | |
| nr file modification | |
| nr file modificatio | |
| nr file modification | |
| nr file modification | |
| or file modification with | |
| nr file modification without nric | |
| nr file modification without nric | |
| nr file modification without | |
| nr file modification without nric | |
| nr file modification without prior written o | |
| nr file modification without nrior writter | |
| nr file modification without prior written o | |
| nr file modification without prior written o | |
| or file modification without prior written concept | |
| or file modification without prior written concept of the | |
| or file modification without prior written concept of t | |

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

| Management Software | | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| User Interface | Native PC application Embedded Webapp CLI | , , | , , | ۰ ۲ | , , | , , | , , | , , |
| 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 lidently-based authentication of user Number of release Number of release Strict Internal separation of users | 2 3 (SMC)/4 (CM7) | 2 3 (SMC)/4 (CM7) | 2 3 (SMC)/4 (CM7) | 2 3 (SMC)/4 (CM7) | 2 3 (SMC)/4 (CM7) | 2 3 (SMC)/4 (CM7) | 2 (SMC)/4 (CM7) |
| Device Management | Device Diagnostics Link Montoring (SNMP) Connection Diagnostics In-band Network Diagnostics Remote Update/Upgrade | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | , , , , , , | , , , , , , | , , , , , , | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ,,,,, |
| Certificate Authority & Management Certificate Certificate | ragement Certificate Creation Certificate Management | , , | , , | | , , | , , | , , | |
| Key Management | Group creation Group isolation Key assignment Fail-over configuration | ,,,, | ,,,, | | | * * * * | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | , , , , |
| Price List Price Encryption Unit (in 6) Per extermal Key Server (in 6); o Required Management Schware Optional SMC Schware 5-10e 5-10e 11-200 unimit | Per external Key Server (in 6) Per external Key Server (in 6); optional, no requirement, starting price Required Management Software Optional SMC Software 1-4 encryptors 5-10 encryptors 11-20 encryptors unlimited | on request on request ON7 included free on request on request | on request on request CM7 included free on request on request | on request on request CM7 included on request on request on request | on request on request CM7 included free on request on request on request | on request on request CM7 included free on request on request | on request on request CM7 included free on request on request | on request On request CMT included free on request on request on request |
| Warranty Period (months) Warranty Coverage Parts & Work Basic Support (9 to 5, e-mail, pho Software updates and upgrades | Parts & Work | ر ۲ ک | \$ 12 | 12 | 12 | 12 | on request | |

| - |
|------|
| 2 |
| |
| മ |
| |
| OD - |
| S |
| |
| ΠŪ. |
| |
| S. |
| Ð |
| 0 |
| |
| - |
| = |
| з. |
| |
| _ |
| |
| |

| Platform used Manboard/Firmware Key Management | Supported Usage Scenarios Single tenant Multi-tenant Self-managed Managed encryption service Managed security service Platform | Supported Networks (Transport of Encrypted Frame) Ethemet (native) MPLS (EcoPLS) IP-4/IP-6 TCP UDP | Supported Networks (Encryption) Ethernet MPLS IPwdIPv6 | VLAN-based Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private Tree (EVP-Tree) Ethernet Virtual Private LAN (EVP-LAN) | Port-based Ethernet Private Line (EP-Line) Ethernet Private Tree (EP-Tree) Ethernet Private LAN (EP-LAN) | Point-to-Point (P2P) Point-to-Multipoint (P2MP) Multipoint (MP) Supported Metro Ethernet Topologies | Virtual Appliance Supported Network Topologies | 10 Mbs 1 Gbps 1 Gbps 10 Gbps 25Gps 40 Gbps 100 Gbps | Line Interface/Supported Line Rates | |
|--|--|---|---|--|---|--|---|---|-------------------------------------|-------------------|
| atmedia/atmedia atmedia | | , | | | | , , , | | ✓ R2445 ✓ R2445 ✓ R2445 | Datacryptor 5100 | |
| atmedia/atmedia atmedia | * * * * * | **** | ~ ~ ~ | • • • | | | l | S.R.145 S.R.145 | Datacryptor 5100 | |
| atmedia/atmedia atmedia | | * * * * * * | | | | | l | ≤/RJ45 ≤/RJ45 ≤/RJ45 | Datacryptor 5200 | _ |
| atmedia/atmedia atmedia | | , , , , , , , | , , , | , , , | | , , , | l | SFP SFP SFP | Datacryptor 5300 | Thales E-Security |
| atmedia/atmedia atmedia | | | | | | , , , | l | V/SFP+ V/SFP+ V/SFP+ | Datacryptor 5400 | |
| atmedia/atmedia atmedia | | | , , , | | | , , , | l | | 40G | |
| atmedia atmedia | | | | , , , | 、、、 | , , , | | VIQSFP28 VIQSFP28 VIQSFP28 VIQSFP28 | 100G Roadmap Q4 2017 | |

| Tunnel (Ethernet) Max. number of pens Max. number of MAC Addresses Max. number of MAC Addresses Max. number of VLAN IDs Integrity protection (agorithm) Authentication length (bytes) Fejalay protection Variable reglay window (size) Counter length (in bytes) Frame overhead authenticated encryption Frame overhead authenticated encryption (AE) Ethernet multi-hop support | Transport (Payload only) Max. number of MAC Addresses Max. number of MAC Addresses Max. number of VLAN IDs Integrity protection Authentication length Optes) Feplay protection Variable encryption offset (fixed) Variable encryption offset (fixed) Variable encryption offset (fixed) Variable encryption offset (fixed) Counter length (in bytes) Frame overhead unauthenticated encryption only) Frame overhead unauthenticated encryption (AE) Ethernet multi-hop support | Latency Latency P2P Mode cut-through store & forward Latency MP Mode cut-through store & forward Encryption Modes Native Ethernet Encryption Frame Encryption (fault - P2P only) Integrity protection (algorithm) Authentication length (bytes) Replay protection Variable replay window (size) Counter length (in bytes) Frame overhead (authenticated encryption) Frame overhead (authenticated encryption) | Data Plane Encryption Standard and Processing Encryption Standard Biock Cipher Key Length (in bit) Processing Method cat-through store&toward Encryption Hardware FIGA ASIC CPU |
|--|--|---|--|
| SS SS SS SS SS SS SS SS SS SS | uninnica 256 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 8/1000 | <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <42,/s <43,/s <43,/s <43,/s <43,/s <43,/s <43,/s <43,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <44,/s <4 | Some Some Some Some Some Some Some Some |
| unlimited unlimited GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | unlimited cocM 8/16 8/16 18/26 ۱8/26 | -2445 -2455 | C C See See See See See See See See See |
| unlimited GCM 8/16 8/303 8/303 8/303 8/303 8/303 8/303 8/30 8/30 | uniimted 256 GCM 8/16 8/16 8/16 18/26 | <42µs <48µs <48µs <48µs 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | C C 256 G AES |
| Construction Co | unlimited unlimited GCM 8/16 8/20s 18/26 | | Thales E-Security GCM 256 |
| unlimited unlimited GCM 8 GCM 8 GCM | uniimted 256 84 84 84 84 84 84 84 84 84 84 84 84 84 | <4/4 8/16 8/16 8/16 8/16 8/16 8/16 8/16 18/26 | 、、、、 226 GAES |
| unlimited unlimited GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 | ۱۹۵۵ unlimited ۵.004 ۱۳۷۹ ۱۳۷۹ ۱۳۷۹ | <4/15 \$ \$ \$ | S S S S S S S S S S S S S S S S S S S |
| unlimited unlimited 8 CM 8 CM 8 CM 8 CM 8 CM 8 CM 8 CM 8 CM | uniinned 256 876 876 876 876 876 876 876 | <i>حيا</i> ه د ج د ج د ج د ج د د د د د د د د د د د د | C C See OAES |

MIX=100%

| Traffic Flow Security | Traffic Masking | Based on VLAN ID and presence of MPLS tag MPLS EOIP IP | Based on presence of MPLS tag MPLS EoIP | Basedon VLAN ID MPLS EOIP IP | Mixed Ethernet, MPLS, EoIP and IP Support | Based on MAC Address Based on YLAN ID Based on Frierkyne Based on Multicaet Group Based on Preserve or MPLS Tag Based on IP Address Based on IP Address Combination of multiple selection criteria | Selective Encryption | Transport Tunnel Mode Maximum number of IP addresses Maximum number of IP addresses Inegrity protection (agorithm) Authentication leight (hytes) Additional Authenticated Data (header) Baplay Protection Variable toplay window (stze) Counter length (in bytes) Packet overhead authenticated encryption (AE) | Supported IP versions IPv4 Supported transmission protocols TCP UDP | Native IP Encryption | Ethernet over IP (CoIP) Tunnel (Ethernet over IP) Max. number of paers Max. number of paers Max. number of VLAN USA Integrity protection (abgorithm) Authentication length bytes) Replay protection Variable replay window (size) Counter length (in bytes) Frame overnead authenticated encryption (AE) Ethernet multi-hop support |
|--|-----------------|---|---|---------------------------------------|---|---|----------------------|--|---|----------------------|---|
| ••••TFS mode only secure based on ASIC or FPGA | | • • • • | | | | ***** | | unimited unimited GCM 8/16 8/16 8/16, IPV6: 58/66 | 、、、、 | | native IP/UDP 2 (r22), 1000 (MP) uniimited GCM 8/16 8/16 8/16 8/16 54/52 |
| t on ASIC or FPGA | | | | | | * * * * * * * * | | unlimited unlimited GCM 8/6 8 0-33 8 9 0-35 8 9 | 、、、、 | | 2 (P2P), 1000 (MP) 2 (P2P), 1000 (MP) unimited GCM 8 (16 8 (16 8 (16 8 (16) 8 (16) 10 (16) |
| ĸ | | | | | | ***** | | unimited unimited SCM 8/6 0.30s 0.40s 1Pv4: 38/46, IPv6: 58/66 | | | native IP/UDP 2 (P2P), 1000 (MP) uninited GCM 8/16 8/16 5/462 |
| 7 | | 、、、 | , , , | , , , | | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | | unlimited unlimited SCM 8/6 0.33 8 8 0.35 8 1P-4: 38/46, IP-6: 58/66 | ,, ,, | | 2 (P2P), 1000(MP) 2 (P2P), 1000(MP) unimited GCM 8 (16 8 (16 8 (16 8 (16 8 (16 8 (16)) 8 (16)) 8 (16)) 8 (16)) 8 (16)) 8 (16)) 8 (16)) 8 (16)) 9 (16)) |
| ĸ | | | | | | ***** | | uniimited uniimited UCM 8/6 8 8 9 8 9 8 9 8 9 | | | 2 (P2P), 1000 (MP) 2 (P2P), 1000 (MP) unimited GCM 8 16 8 16 8 16 54/82 54/82 |
| ĸ | | | | | | ***** | | unlimited unlimited SCM 8/6 0.30s 0.40s 0.40s | 、、、、、 | | 2 (P2P), 1000 (MP) 2 (P2P), 1000 (MP) uninited GCM 8 (16 8 (16 8 (16 8 (16) 8 (16) 10 (16 |
| ۲. | | | | | | ***** | | unimited unimited GCM 8/16 0-30s 8 1Pv4: 38/46, IPv6: 58/66 | ,, ,, | | native IP/UPP 2 (P2P), 1000 (MP) unlimited GCM 8/16 8/16 8/16 8/16 8/16 8/16 8/16 8/16 |

Thales E-Security

*IMIX=100%

| Session Key (DEK) Exchange Agreement Session Key (DEK) Exchange Frotocol Automatic Change of Session Key Minimum Time Interval for Session Key Change (min) | Matter Key (KEK) Agreement Matter Key (KEK) Agreement Automatic Change of Matter Key Mimmum suggested Time Interval for Master Key Change (min) Separate Master Key (KEK) per group Separate Master Key (KEK) per group | Key Agreement and Key Exchange | Ad-hoc authentication of peers (manual) Signature key protocol | Asymmetric Signature: Certificate Maximum number of certificates per encorptor Key lenght | Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encryptor Key length | Device Authentication | CBC-MAC-GCM Key length | SHA-2 Key length | Hash Algorithms | Supported Curves: NIST Branpool Custom Curves | Elliptic Curve Cryptography (ECC) Key length | RSA Key length | Asymmetric Key Algorithms (Public Key Cryptography) | Hardware Random Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) | Key Generation and Storage | Key Management | Autonomous operation | Integrated Key Server Support for external Key Server External Key Server Support for multiple distributed Key Server Support for fail-over to back-up Key Server | Key Server | Auto-discovery of network encryptons Auto-discovery of key servers Auto-discovery of VLANs Disabling of auto-discovery | Auto-discovery |
|--|--|--------------------------------|---|---|---|-----------------------|------------------------|------------------|-----------------|---|---|-------------------|---|---|----------------------------|----------------|----------------------|---|------------|---|-------------------|
| atmedia atmedia 1 | ECKAS-DH**** atmedia 60 | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | TE/TP | | | ٢ | ,, ,, | | ,,,, | |
| atmedia 1 • | ECKAS-DH | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | | 512/521 | NVA | | TE/TP | | | ۲ | 、、、、 | | * * * * | |
| atmedia 1 | ECKAS.DH***** atmedia 60 | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | TE/TP | | | ٢ | ,, ,, | | ,,,, | |
| atmedia 1 | ECKAS.DH | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | TE/TP | | | ٢ | ,, ,, | | ,,,, | Thales E-Security |
| atmedia 1 | ECKAS-DH | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | TE/TP | | | ٢ | ,, ,, | | ,,,, | |
| atmedia 1 | ECKAS.DH | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | TE/TP | | | ۲ | ,, ,, | | ,,,, | |
| atmedia atmedia | ECKAS.DH**** | | AES-MAC/ECDSA**** | optional 64 (recommended:18) 512 | 512 (recommended:18) 256 | | 256 | 512 | | ,,, | 512/521 | N/A | | ч | | | ۲ | ,, ,, | | ,,,, | |

***ECDSA optional for use with optional certificates
***** NIST, Brainpool or custom curves with 256 to 521 bit length

| Group Key Distribution Unclast (unique KEK per group member) Broadcast (same KEK for all group members) | Exclusion MAC address VLAN ID Frames with MPLS tag IP Address IP Multicast Group | Additional separate authentication per group Group Membership Definition Multicast group membership Individual membership VLAN membership Trunked VLAN membership IP Address | individual key per broadcast group Individual key per broadcast group (VLAN ID) | Key assignment based on: MAC address (pairwise and mixed) Multicast groups (mixed) VLAV ID (group) Port Group (group) IP Address IP Address | Multipoint Key System Supported key systems: Group Mixed (pairwise unicast, group multicast) | Key assignment based on: VLANID Port Group IP Address | Point-to-Multipoint Key System Supported key systems: Painvise Group | Key assignment based on: VLANID Port Group IP Address | Key System Point-to-Point Key System Supported key system Pairwise Group |
|---|--|--|--|--|---|---|---|---|--|
| | **** | , | ~ ~ | | Bidirectional Group | ,,,,, | Sidirectional Group | ,,,,, | Bidrectional Group |
| , , | ,,,,, | | , , | | Bidirectional Group | ,,,,, | S Bidirectional Group | ,,,,, | Bidirectional Group |
| , , | ,,,,, | ***** | , , | | Bidirectional Group | ,,,,, | √ Bidirectional Group | ,,,,, | K Bidfrectional Group |
| , , | * * * * * | , | < < | | Sidirectional Group | ,,,,, | S Bidirectional Group | ,,,,, | Bidirectional Group |
| ~ ~ | **** | ***** | | | Sidirectional Group | ,,,,, | S Bidirectional Group | * * * * * | Selfrectional Group |
| ~ ~ | * * * * * | | < < | | Sidirectional Group | * * * * * | S Bidirectional Group | * * * * * | Bidirectional Group |
| | **** | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ~ ~ | | Bidirectional Group | **** | Sidirectional Group | **** | Bidirectional Group |

Thales E-Security

| * Products using the platform have BSI VS-NfD, NATO restricted, EU Restrint (including 2nd Evaluation by NL) approvals | Boot Time Cold boot until operational Warm boot until operational | Security Approvais * Safety Approvals | MTBF Tamper Security | Redundant, hot-swappable power supply High Availability functionality (two-node cluster) | Physical Device Access Redundant Power Supply | Height in 19" Rack Number of external encrypted Ethernet ports | Unit | Syslog Support (Server) | Event Log (local) Audit Log (local) | Logs | Remote Monitoring (SNMP) | Proprietary | SNMP (read-onlyread-write) TLS | | In-band Management | Smart Card (Secure Card) Support USB Port | Separate Ethernet port | Out-of-band Management | IPv4 IPv6 | System Configuration and Management Access | | Dead Peer Detection Optical Loss Pass-Through Link Loss Carry Environ | Point-to-Multipoint Multipoint | Ethernet Fragmentation/Defragmentation Point-to-Point | Ethemer Flow Control Via PAUSE | Jumbo Frame Support | Dump in the Wire deployment | Network Support |
|--|---|--|-------------------------|---|--|---|------|-------------------------|--|------|--------------------------|-------------|-----------------------------------|----------|--------------------|--|------------------------|------------------------|--------------|--|-------|---|-----------------------------------|--|--------------------------------|---------------------|-----------------------------|--------------------|
| icted, EU Restrint (including 2nd Evalu | 25s 27s | FIPS 140-2 L3 in progress | > 50.000h TE/TP | 13 | back | 1 U | | ۲ | , , | | VZG/V3 | • | read-only | • و | ۲, | ۲, | < < | . . | , , | Ī | | NIA S | , , | , , | • | | | |
| ration by NL) approvals | 25s 27s | FIPS 140-2 L3 in pro | | 1:1 | back | - ē | | ٢ | ۰ ۲ | | V/2C/V3 | • | read-only | • | ۲ | ۲ | < < | | , , | | | , NA | 、、 | 、、 | < | | • | |
| | 25s 27s | gress FIPS 140-2 L3 in progress FIPS EN55032 Class B, FCC Part 15 Class B, ROHS | > 50.000h ТЕЛТР | ± < | front | → ć | | ٢ | 、、 | | V/2C/V/3 | ~ | read-only | , | ۲ | ۲ | , , | | , , | | | NIA S | 、、 | 、、 | • | | | |
| | 25s 27s | FIPS 140-2 L3 in progress ROHS | > 50.000h TE/TP | ∃ < | front | 1 10 | | ۲ | , , | | VZC/V3 | • | read-only | , | < | ۲ | < < | | ς ς | | | | , , | , , | < | | | I nales E-Security |
| | 25s 27s | FIPS 140-2 L3 in progress | > 50.000h TE/TP | ₫ ヽ | front | 1 1 | | ٢ | <i>د د</i> | | V2C/V3 | ~ | read-only | , | ۲ | ۲ | < < | | ~ ~ | | | | 、、 | , , | < | | ÷ | |
| | 25s 27s | FIPS 140-2 L3 iplanned | > 50.000h TE/TP | ₫ < | front ر | 1- ⊂ | | ۲ | <i>د د</i> | | VZC/V-3 | • | read-only | < | < | | < < | | ς ς | | 11011 | 2 7 7 | , , | , , | < | | ¢ | |
| | 25s 27s | FIPS 140-2 L3 planned | > 50.000h TE/TP | ± ₹ | front | 1-4 C | | ۲ | 、、 | | VZC/V3 | • | read-only | • ح | ۲ | ~ ~ | , , | | , , | | 1.001 | N ((| , , | 、、 | | | | |

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

Thales E-Security

| Warranty Period (months) Warranty Coverage Parts & Work Basic Support (9 to 5, e-mail, phone) Software updates and upgrades Warranty Extension (per year) | Price List Price Encryption Unit (in 6) Per external Key Server (in 6); optional, no requirement Required Management Software 2-10 encryptors 11-25 encryptors 26-50 encryptors 51+ encryptors | Certificate Authority & Management Certificate Creation Certificate Management Group creation Group isolation Key assignment Fall-over configuration | Device Management Device Diagnostics Link Monitoring (SNMP) Connection Diagnostics In-band Nework Diagnostics Remote Update/Upgrade | Management Access Role-based access Identity-based authentication of user Number of hierarchy levels Number of roles Strict internal separation of users | Initial Device Set-up Local (out-of-band) Remote (out-of-band) Local (out-of-band) Remote (in-band) Remote (out-of-band) | Management Software User Interface Native PC application Embedded Webapp CLI |
|---|---|--|--|---|---|--|
| 24 on request on request on request | on request on request included included included | optional optional cytional | ,,,,, | ζ σ Ν ζ ζ | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | , , |
| 24 on request on request on request | on request on request included included included | optional optional | ,,,,, | ζσΝζζ | ,,,,,,, | , , |
| 24 on request on request on request | on request included included included | optional optional solutional | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | ζσΝζζ | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | |
| 24 on request on request on request | on request on request included included included | optional optional | ,,,,, | ζσΝζζ | *** ** | < < |
| 24 on request on request on request | on request on request included included included | optional optional optional | * * * * * | ₹ 07 № ₹ | *** ** | 、 、 |
| 24 on request on request | on request on request included included included | optional optional | ,,,,, | ζσΝζζ | *** ** | < < |
| 24 on request on request | on request on request included included included | optional optional | ,,,,, | ζσΝζζ | ,,,,,,, | |

Thales E-Seccurity

92007 - 2017 Christoph Jaggi ALL RIGHTS RESERVED

| Platform used Mainboard/Firmware Key Management | Self-managed Managed encryption service Managed security service Platform | Single tenant Mult-tenant | Ethemet (native) MPLS (EoMPLS) IPv4/IPv6 TCP UDP UDP | Supported Networks (Transport of Encrypted Frame) | Supported Networks (Encryption) | VLAN-based Ethernet Virtual Private Line (EVP-Line) Ethernet Virtual Private Tree (EVP-Tree) Ethernet Virtual Private LAN (EVP-LAN) | Port-based Ethernet Private Line (EP-Line) Ethernet Private Tree (EP-Tree) Ethernet Private LAN (EP-LAN) | Supported Metro Ethernet Topologies | Point-to-Point (P2P) Point-to-Multipoint (P2MP) Multipoint (MP) | Supported Network Topologies | Virtual Appliance | 10 Mbs 100 Mps 1 Gbps 10 Gbps 25Gps 40 Gbps 100 Gbps | Line Interface/Supported Line Rates | |
|---|--|------------------------------|---|---|---------------------------------|--|---|-------------------------------------|---|------------------------------|-------------------|--|-------------------------------------|--------|
| ViaSat/ViaSat MKA/EAPOL-TLS | Roadmap Q4 CY 2017 Roadmap Q4 CY 2017 | ٢ | Roadmap 04 CY 2017 Roadmap 04 CY 2017 | ς, | | , , , | , , , | | | | ۲ | ,,, | SEC-1140V | Via |
| ViaSat/ViaSat MKA/EAPOL-TLS | Roadmap Q4 CY 2017 Roadmap Q4 CY 2017 | ٢ | Roadmap C4 CY 2017 Roadmap C4 CY 2017 | . . | | | | | | | | VSFP+ VSFP28 VGSFP28 | SEC-1170 | Viasat |
| | | | EolP only EolP only | | | | | | | | l | | | |

| Tunnel (Ethernet) Max. number of beers Max. number of MAC Addresses Max. number of MAC Addresses Integrity protection (agorithm) Authentication leagth (tytes) Replay protection Variable replay window (size) Counter length (in tytes) Frame overhead authenticated encryption Frame overhead authenticated encryption (AE) Ethernet multi-hop support | Transport (Payload only) Max. number of peers Max. number of MAC Addresses Max. number of MAC Addresses Max. number of MAC Addresses Max. number of VLAN Ds Integrity protection Variable encryption (siget) Definable encryption offset (fixed) Variable encryption offset (fixed) Counter length (fit ybres) Frame overhead authenticated encryption (AE) Ethernet multi-hop support | Native Ethernet Encryption Frame Encryption (Bulk - P2P only) Integrity protection Aurhentcation length (bytes) Replay protection Variable replay window (size) Counter tength (in bytes) Frame overhead (authentizated encryption) Frame overhead (authentizated encryption) Ethernet multi-hop support | Encryption Modes | Latency P2P Mode cut-through store & forward Latency MP Mode cut-through store & forward | CPU Latency | Encryption Hardware FPGA ASIC | Processing Method cut-through store&flow.ard | Encryption Standard Block Cipher Pretered Mode of Operation Alternative Mode of Operation Key Length (in bit) | Data Plane Encryption Standard and Processing |
|---|--|--|------------------|---|----------------|-------------------------------------|--|---|---|
| | 32 - Expandable to 256 unlimited GCM 56 ≤ 2/31-1 framestime 8 8 8 | | | NA NA | ĸ | | ۲ | AES GCM 256 | Via |
| | 32 - Expandable to 256 unimitad unimited GOM 16 \$ 2131-1 framestime \$ 2.31-1 framestime \$ 3.2 \$ 3.2 \$ | | | <3µs | | ۲ | ۲ | AES GCM 256 | Viasat |

| Traffic Flow Security | Traffic Masking | Based on VLAN ID and presence of MPLS tag MPLS EcilP IP | Based on presence of MFLS tag MPLS EcilP IP | Based on VLAN ID MPLS EoIP IP | Based on MAC Address Based on VLAV ID Based on Ethertype Based on Muticaat Group Based on Peenze of MPLS Tag Based on IP Address Combination of multiple selection criteria Mixed Ethernet, MPLS, EoIP and IP Support | Selective Encryption | Transport/Tunnel Mode Miximum number of pers Maximum number of IP addresses Maximum number of IP addresses Inegrity protection (algorithm) Authentication (arght (tyres) Additional Authenticated Data (header) Replay Protection Variable replay window (size) Counter length (in bytes) Packet overhead authenticated encryption (AE) | Supported IP versions IP/4 Supported transmission protocools TCP UDP | Native IP Encryption | Supported transmission protocols (UDP/TCP) Max. number of peers Max. number of MAC. Addresses Max. number of VLAN IDs Integrity protection (agorithm) Authentication length (bytes) Replay protection Variable replay window (size) Counter length (in bytes) Counter length (in bytes) Frame overhead authenticated encryption Frame overhead authenticated encryption Frame invalidation of the support | Tunnel (Ethernet over IP) | Ethernet over IP (EoIP) |
|-----------------------|-----------------|--|--|--|--|----------------------|---|--|----------------------|---|---------------------------|-------------------------|
| Roadmap Q4 CY2017 | | Roadmap Q4 CY2017 | Roadmap Q4 CY2017 | Roadmap Q4 CY2017 | | | | | | | Roadmap Q4 CY2017 | Viasat |
| Roadmap Q4 CY2017 | | Roadmap Q4 CY2017 | Roadmap Q4 CY2017 | Roadmap Q4 CY2017 | | | | | | | Roadmap Q4 CY2017 | at |

| Key Agreement and Key Exchange Master Key (KEX) Agreement Master Key (KEX) Cargener Automatic Change of Master Key Minimum suggested The Interval for Master Key Change (min) Separate Master Key (KEK) per group Separate Master Key (KEK) per group Sesion Key (CEK) Exchange Agreement Sesion Key (CEK) Exchange Protocol Automatic Change of Sesion Keys Change (min) | Maximum number of certificates per encryptor Key lenght Advice authentication of peers (manual) Signature key protocol | SHA-2 Key length Device Authentication Symmetric Signature: Pre-shared Key (PSK) Maximum number of PSKs per encryptor Key length | Hash Algorithms | RSA Key length Elliptic Curve Cryptography (ECC) | Key Generation and Storage Hardware Random Number Generation Tamper Security Key Storage (tamper-evident or tamper-proof) Asymmetric Key Algorithms (Public Key Cryptography) | Support for external Key Server External Key Server Support for multiple distributed Key Servers Support for fail-over to back-up Key Server Aubnomous operation Key Management | Auto-discovery Auto-discovery of network encryptors Auto-discovery of key servers Auto-discovery of VLAts Disabing of auto-discovery Key Server Integrated Key Server |
|--|---|--|-----------------|---|--|--|---|
|--|---|--|-----------------|---|--|--|---|

| ۲ | Roadmap 04 CY2017 | K Roadmap Q4 CY2017 | ۲, | , , | Via |
|---|-------------------|------------------------|----|-----|--------|
| ۲ | Roadmap Q4 CY2017 | Roadmap Q4 CY2017 | ۲ | , , | Viasat |

| ۲ | 384 | | N/A | (dependent on CPU) |
|---|-----|--|--|--|
| ۲ | 384 | | TE/TP | ۲ |
| | | | VNF requires intel RDRAND (Hardware TRNG) built into all Xeons | |

| CDSA W/SHA384 | x.509 1 | 512 256 | |
|---------------|---|--|--|
| CDSA W/SHA384 | x.509 1 | 512 256 | |
| | Certificates used for asymmetric exchange and key derivation exchange Only 1 certificate currently supported - due to market re-analyzing when multi-tenant support will be added. | Connectivity Association Key (CA), also used for Key derivation to get SAKs and KEKs 256-bit CAKs and a 128-bit CAK-Name (CKN) which is cryptographically derived from the CAK. | |

512

512

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

тьз. 5 **с б**ар 5 **с б**ар 5 **с б**ар

| Group Key Distribution Unicast (unique KEK per group member) Broadcest (same KEK for all group members) | Exclusion MAC address VLAN ID Frames with MPLS tag IP Address IP Mutcast Group | Group Membership Definition Multicast group membership Individual membership Network membership VLAN membership IP Address | Group Key System Specifics Additional separate authentication per group | Individual key per multicast group Individual key per broadcast group (VLAN ID) | Key assignment based on: Multicast groups (mixed) VLAN ID (group) Port Group (group) IP Address IP Multicast Group | Supported key systems: Pairwise Group Mixed (pairwise unicast, group multicast) | Multipoint Key System | Key assignment based on: MAC Address VLAN ID Port Group IP Address | Supported key systems: Pairwise Group | Point-to-Multipoint Key System | Key assignment based on: MAC Address VLAN ID Port Group IP Address | Supported key system Pairwise Group | Point-to-Point Key System | Key System |
|---|--|---|--|--|--|--|-----------------------|---|---|--------------------------------|---|---|---------------------------|------------|
| ers) | Roadmap 02 2017 | | <. | 、 、 | | Unidirectional Group | | | Unidirectional Group | | | Unidirectional Group | | <u></u> |
| | Roadmap O2 2017 | | ۲. | | **** | Unidirectional Group | | **** | Unidirectional Group | | **** | Unidirectional Group | | Viasat |

| Boot Time Cold boot until operational (P2P) Warm boot until operational (P2P) | Height in 19" Rack Number of external encrypted Ethernet ports Physical Device Access Redundant Power Supply Redundant, hot-swappable power supply High Availability functionality (two-node cluster) MTBF Tamper Security Security Approvals Safety Approvals | Logs Event Log (local) Audit Log (local) Systog Support (Server) Unit | In-band Management SHH SSIMP (read-only/read-write) TLS Proprietary Remote Monttoring (SNMP) | IPv4 IPv6 Out-of-band Management RS-232V.24 Separate Ethernet port Smart Card (Secure Card) Support USB Port | Deed Peer Detection Optical Loss Pass-Through Link Loss Carry Forward System Configuration and Management Access | 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 |
|---|---|---|---|--|---|---|
| 560s | N/A N/A 1-1 N/A | ,,, | Roadmap Q3 C | , , , | , | , , , |

Viasat

| ۲, | |
|----|-----|
| ۲ | ,,, |

| 5 | Roadmap Q3 CY2017 | , , | ۲ |
|---|-------------------|-----|---|
| 6 | Roadmap Q3 CY2017 | , , | ۲ |

| | N/A | ÷. | | N/A | unrestricted |
|--|-------|-----|---|-------|--------------|
| FIP5-140-2 Level 3 CY2017, NIAP/CC EAL-4 All planned; FIP5 is in process. EN55022 class B - FCC Part 15 Class B | ТЕ/ТР | 1-1 | ٢ | front | up to 4 |
| All planned; FIPS is in process. | | | | | |

120s 120s

-

, , ,

| | | Price | Key Management | Certificate Authority & Management | Device Management | Management Access | Device Configuration | Initial Device Set-up | User Interface | Management Software |
|----|---|-------|---|---|--|--|---|---|---|---------------------|
| | 1G VNF, or 10G SEC-1170 4x10G,4x25G 100G 2-10 encryptors 11-25 encryptors 28-50 encryptors 28-50 encryptors 51+ encryptors | | Group creation Goup isolation Key assignment Fail-over configuration | t Certificate Creation Certificate Management | Device Diagnostics Lunk Monitoring (SNMP) Connection Diagnostics In-band Network Diagnostics Remote Update/Upgrade | Role-based access identity-based authentication of user Number of hierarchy levels Number of roles Strict internal separation of users | Local (out-of-band) Remote (in-band) Remote (out-of-band) | Local (out-of-band) Remote (out-of-band) | Native PC application Embedded Webapp CLI | |
| 12 | on request | | | Roadmap O2 CY2017 Roadmap O2 CY2017 | ,,,,, | ς Ν ω ς ς | ۲ | 、、 | 、、 | Viasat |
| 12 | on request on request on request | | | Roadmap Q2 CY2017 Roadmap Q2 CY2017 | | ς Ν ωςς | ۲ | , , | | sat |

© 2007 - 2017 Christoph Jaggi ALL RIGHTS RESERVED Absolutely no re-publishing, distribution or file modification without prior written consent of the auth www.uebermeister.com