SENETAS ENCRYPTION KEY MANAGEMENT

STATE-OF-THE-ART KEY MANAGEMENT FOR ROBUST NETWORK SECURITY

WHO SHOULD READ THIS DOCUMENT

System Integrators, Cloud and Data Centre Service Providers, Layer 2 Data Networks Managers, Network Architects, Network Engineers, Data Security Managers and Staff, Chief Information Officers, Chief Information Security Officers, Data Security and Network Procurement Staff.

KEYWORDS

Encryption Key Management, High Assurance Encryption, Layer 2 Data Networks, Robust Encryption, Ethernet Networks, High-Speed Data Networks, Network Data Security, Encryption Security, Network Encryption, Certified Encryption, Encryption Authentication, Encryption Hardware, Data Plane Information, MAC Header, SecTag, Secure Keys, Entropy, Certificate Authority, Public Key Algorithms, Pairwise Key System, Group Key System, Multicast Encryption.

SENETAS

Security without compromise

Encryption Key Management is a crucial component of any robust encryption security solution for today's high-speed networks.

WHEN IT COMES TO NETWORK ENCRYPTION SECURITY, THERE ARE TWO BASIC GRADES - HIGH ASSURANCE AND LOW ASSURANCE.

High Assurance solutions are those typically demanded by government agencies and corporations transmitting sensitive or confidential data.

The level of data sensitivity usually mandates that any solution is required to have certified encryption components.

High Assurance solutions are commonly known as "robust" encryption. To be truly robust or high assurance, an encryption security product requires four key components:

> Certification as being suitable for government and defence use by a recognised authority (EG. Common Criteria, FIPS, NATO or CESG)

> Standards-based encryption algorithm (EG. AES 256).

> Client-side encryption key management, where encrypted keys and encryption authentication is only accessible by the client.

> End-to-end encryption, where there is no point in the network where un-encrypted data is accessible.

WHAT IS ROBUST ENCRYPTION?

There are numerous encryption solutions available today; both hardware and software-based. Some are designed specifically to protect "static" data at rest. Others are designed to protect data in motion as it travels across local and wide area networks.

Robust encryption solutions have been available for a number of decades and governments around the world have been their largest single beneficiary.

In fact, it was governments' demand for robust encryption that triggered many vendors to invest in developing encryption technology in the first place.

An essential component of so-called "unbreakable" encryption is that the encryption keys themselves should not be accessible to anyone but the owners of the encrypted data.

If the encrypted encryption keys are securely stored client-side, no matter what type of breach occurs, unauthorised parties can only access the data in its encrypted form.

True to the saying: "Never leave the keys under the mat", the same advice applies to data encryption. When encryption keys are exposed to access by unauthorised parties, the solution is greatly weakened. It is no longer a robust security solution.

Because the robust encryption solution is also providing true end-to-end encryption security, there is no weak point. Even if a router or switch (as is frequently the case) is found to have weak-points or vulnerabilities to attacks, the data passing through those vulnerable devices is always encrypted.

This paper deals with one of the core components of high assurance encryption: Encryption Key Management.

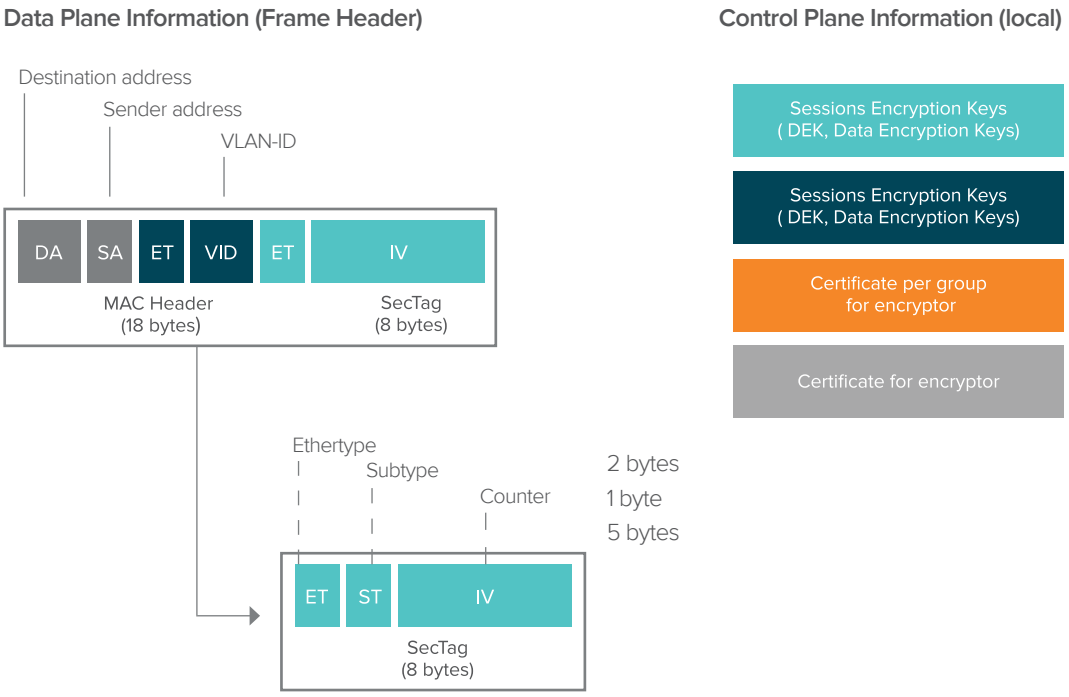
1. INTRODUCTION

An encrypted high-speed data network's robustness is in a large part determined by the type of encryption key management. Ensuring that the transmitted data's encryption keys are not accessible to an unauthorised party is essential to ensuring that a network breach will only result in meaningless data in the hands of an unauthorised party.

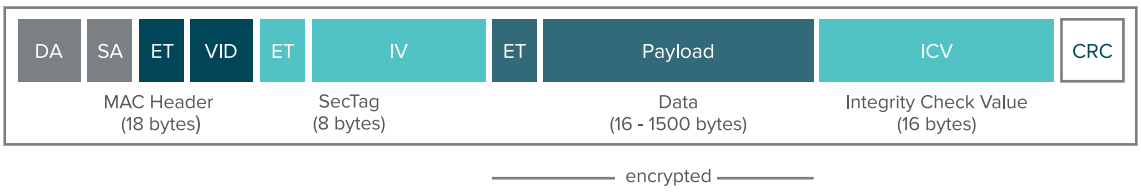
This paper details the state-of-the-art key management system used by Senetas high assurance dedicated encryptors.

2. ENCRYPTION

The encryption and decryption of a frame uses different elements. Some of them are local on the encryptor and the other ones are carried along in the frame header of the encrypted frame. The combination of the two is needed to encrypt and decrypt a frame. The information carried in the header is also used for key assignment.



An encrypted frame during transit has a SecTag and the ICV added while the payload is encrypted.



Encryption depends on key management to the local information needed to encrypt and decrypt frames.

Senetas uses a hybrid approach and combines the advantages of asymmetrical and symmetrical cryptography.

3. KEYS

3.1. SECURE KEYS

Secure encryption depends on key security in all phases:

> A safe key requires entropy (randomness). Whilst both hardware and software can be used to create random numbers, true randomness comes from a hardware source.

> The encryption keys are in plain text while encrypting and decrypting and are dependent on a safe encryption environment. Senetas encryptors feature a tamper-proof enclosure. Any tampering inevitably leads to the zeroization of all data in memory, including the keys in use.

> Keys need to be secure while being transported between encryptors. Keys are always encrypted while in transit.

3.2. KEY BUILD-UP

Each encryptor has its own certificate, issued by the Certificate Authority (CA). The certificate is, initially, secret. Its public key is used as a digital signature, so the recipient can verify the sender.

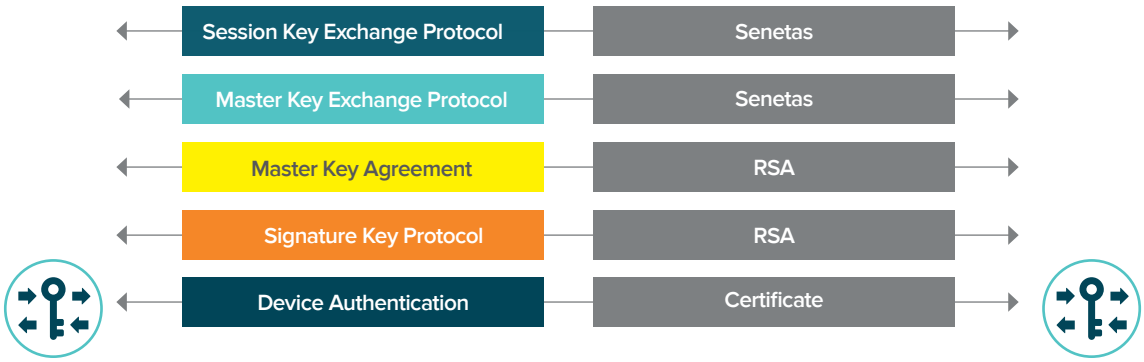
The key exchange uses the certificate to sign the keys (or partial keys) that are exchanged, ensuring that they are coming from the correct remote device.

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.

Subsequently, the encryptor internally generates the master key and encrypts it with the shared secret. The encryptor also generates the session key and uses the master key to encrypt it. The transmission of the master and session keys from one encryptor to the other is always encrypted.

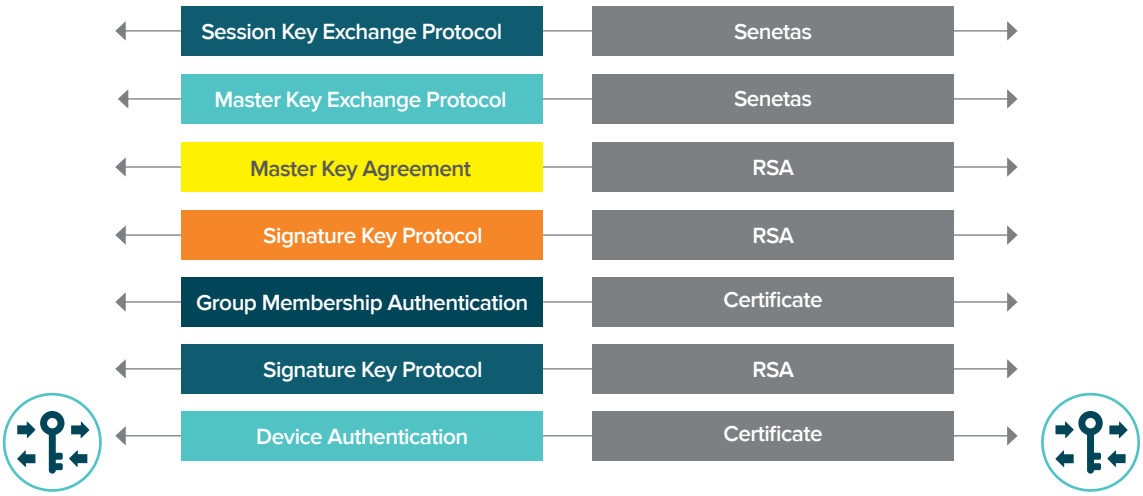
Senetas supports the two leading public key algorithms, RSA and ECC (elliptic curve cryptography), for the exchange of the master keys (key encryption keys). In case of ECC, ECDSA (elliptic curve digital signature algorithm) and ECKAS-DH (elliptic curve key agreement scheme) are used.

The key build-up if RSA is used:

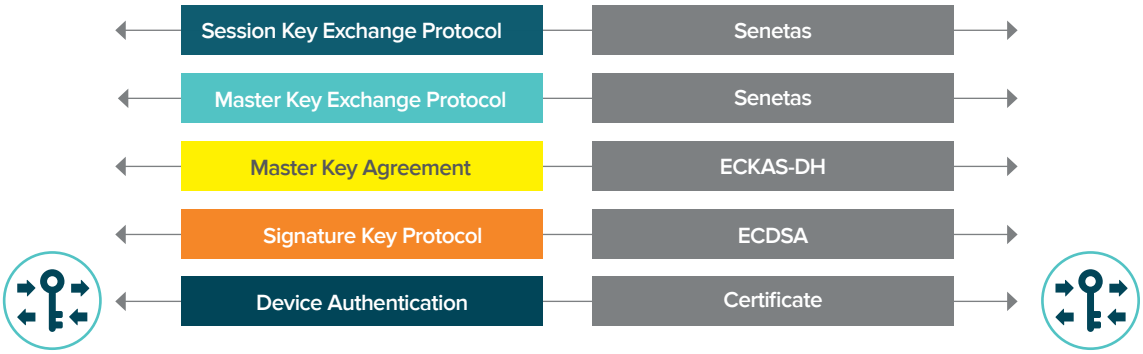


SENETAS
Security without compromise

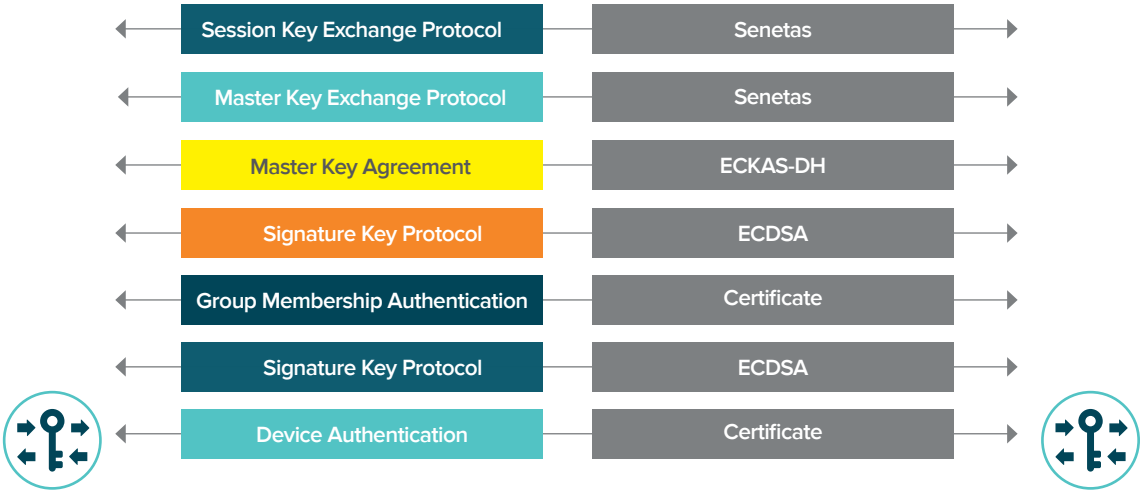
The build-up of group keys adds an additional authentication per group:



The key build-up if ECC (elliptic curve cryptography) is used:



For each group keys there is also an additional level of authentication:

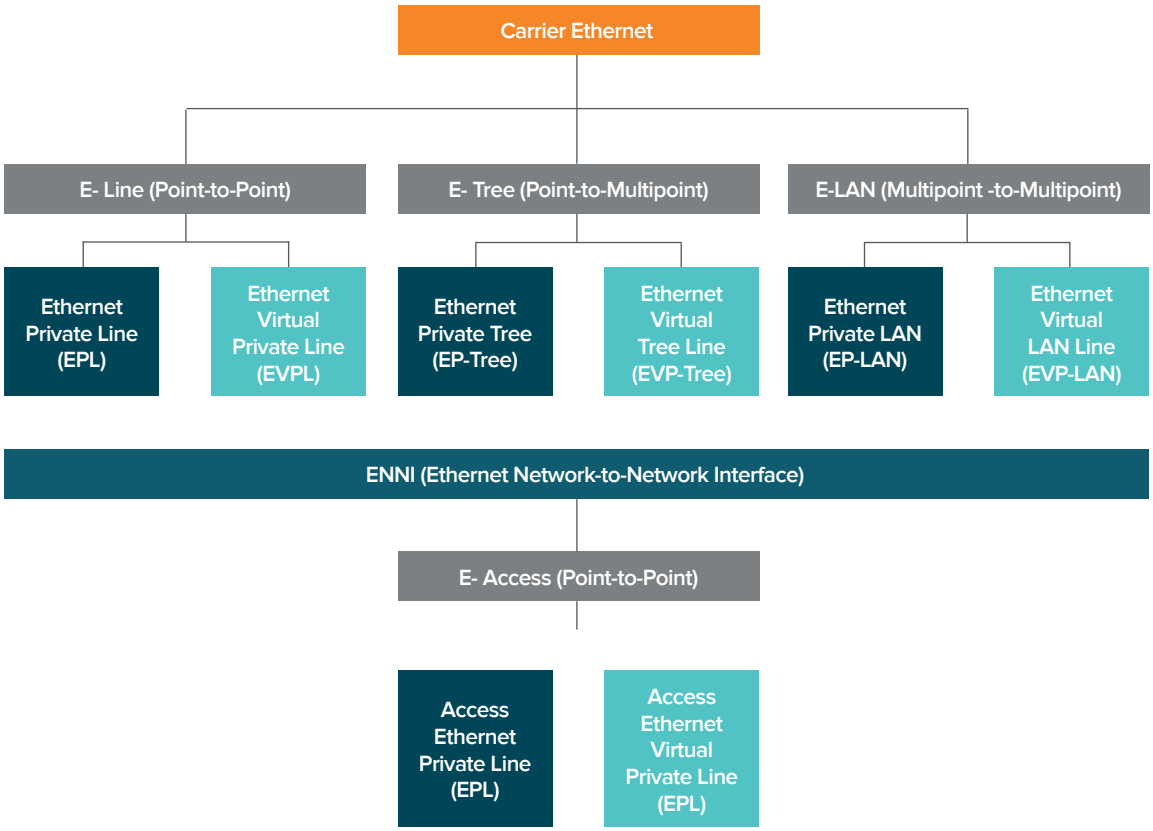


SENETAS
Security without compromise

3.3. KEY SYSTEMS

Senetas offers users a choice of two key systems; pairwise key system or group key system (or a combination of both) in order to accommodate different topologies and usage scenarios.

Metro and Carrier Ethernet comes in three different topologies: point-to-point, point-to-multipoint and multipoint-to-multipoint. Each of these topologies comes in two variants: a port-based one and a VLAN-based one.



Private: Port-based, one EVC per UNI

Virtual: VLAN-based, multiple EVCs per UNI

PAIRWISE KEY SYSTEM

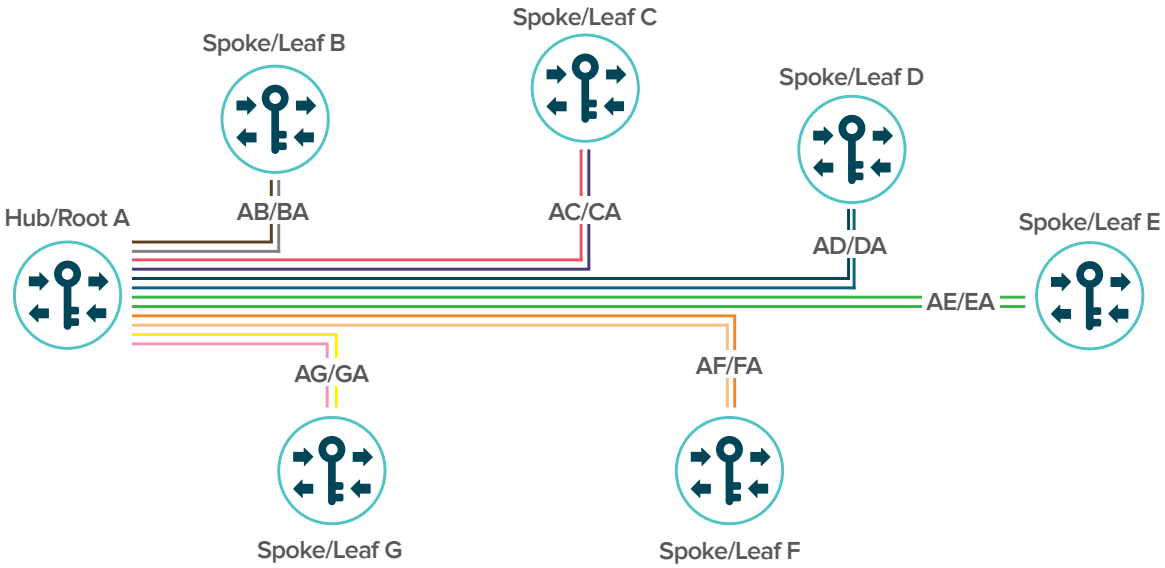
Pairwise Key Systems are designed for point-to-point connections and treat point-to-multipoint and multipoint networks as an accumulation of point-to-point connections.

POINT-TO-POINT (E-LINE)

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.

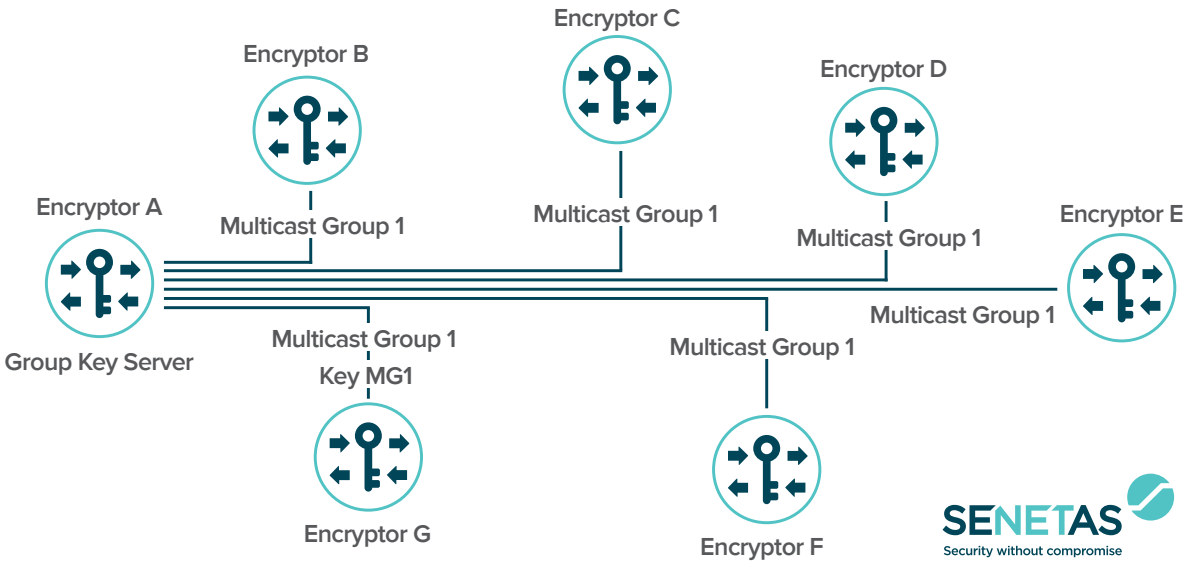
POINT-TO-MULTIPOINT (E-TREE)

A pairwise key system is also well-suited for a point-to-multipoint topology if the network is set up as an accumulation of separate point-to-point links in a hub and spoke configuration.



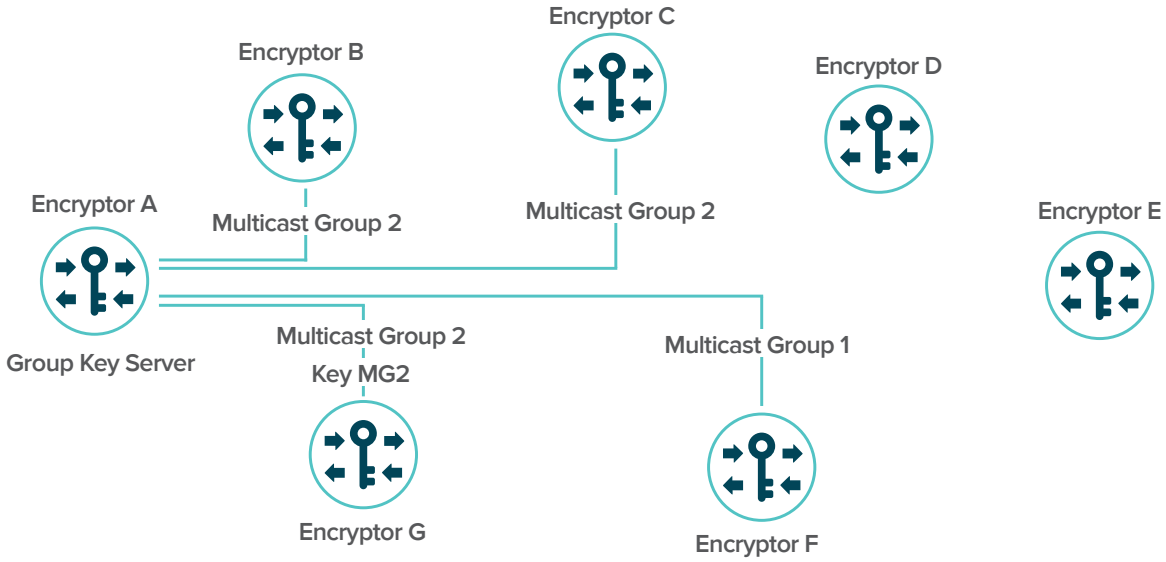
Senetas key management supports the combination of a pairwise key system with a group key system, so multicast frames can be encrypted with a group key when using a point-to-multipoint topology. For unicast frame encryption, pairwise keys are used; while multicast frames are encrypted using the group key system.

A multicast group can comprise all spokes:



SENETAS
Security without compromise

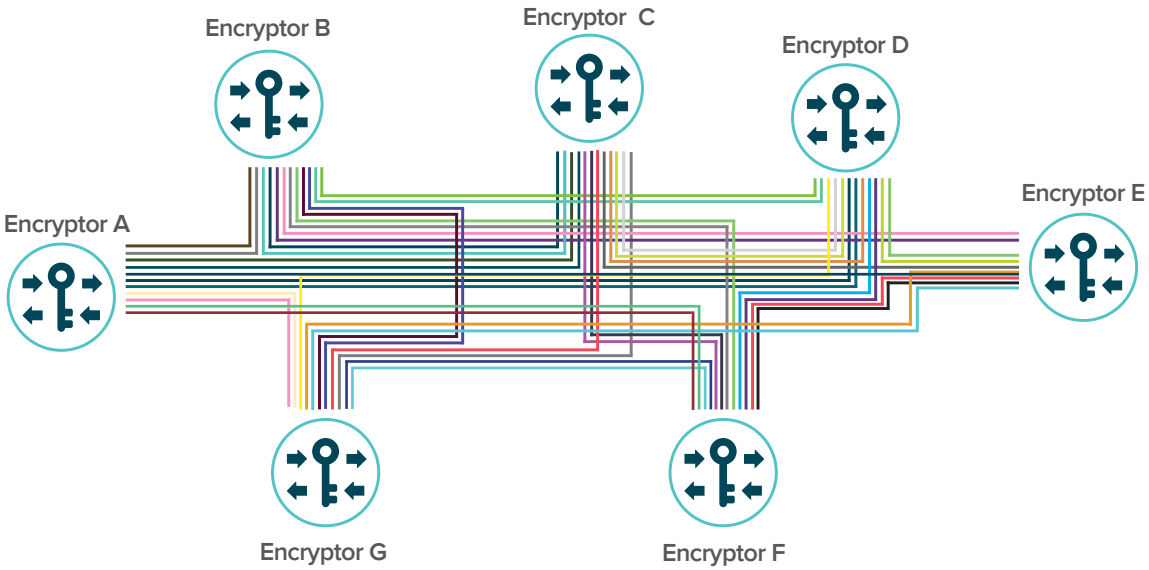
Or a multicast group can comprise only a subset of spokes:



Each multicast group has its own key and up to 256 individual multicast groups are supported. Broadcast frames are treated as a "special case" of multicast and are all encrypted using the same broadcast key.

MULTIPOINT-TO-MULTIPOINT (E-LAN)

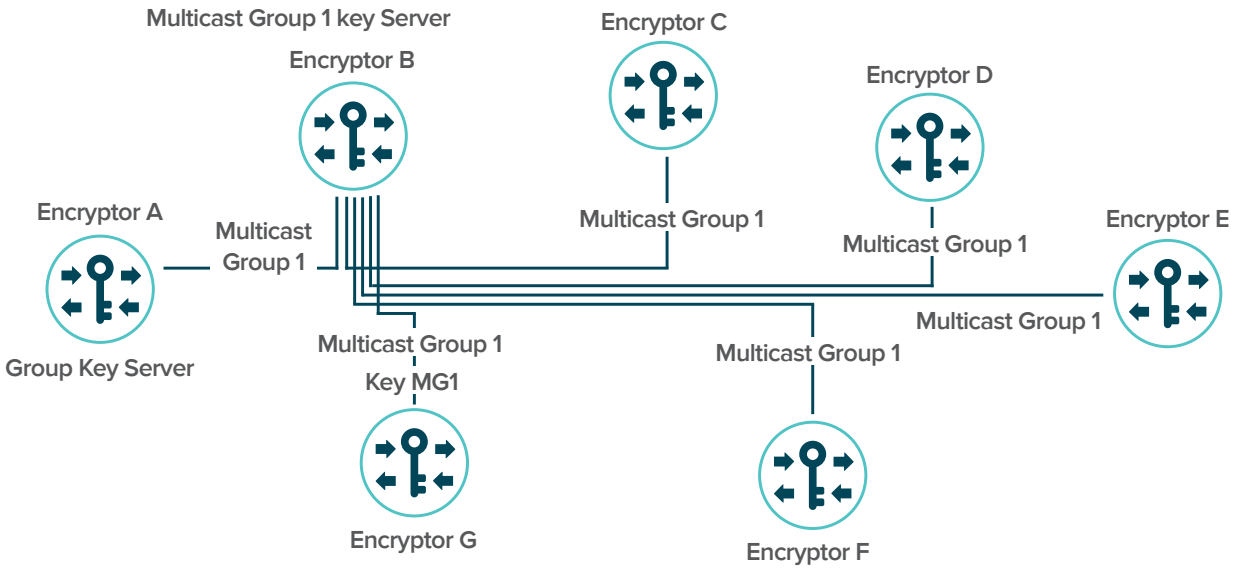
Pairwise key systems also treat multipoint-to-multipoint topologies the same way they treat point-to-point connections.



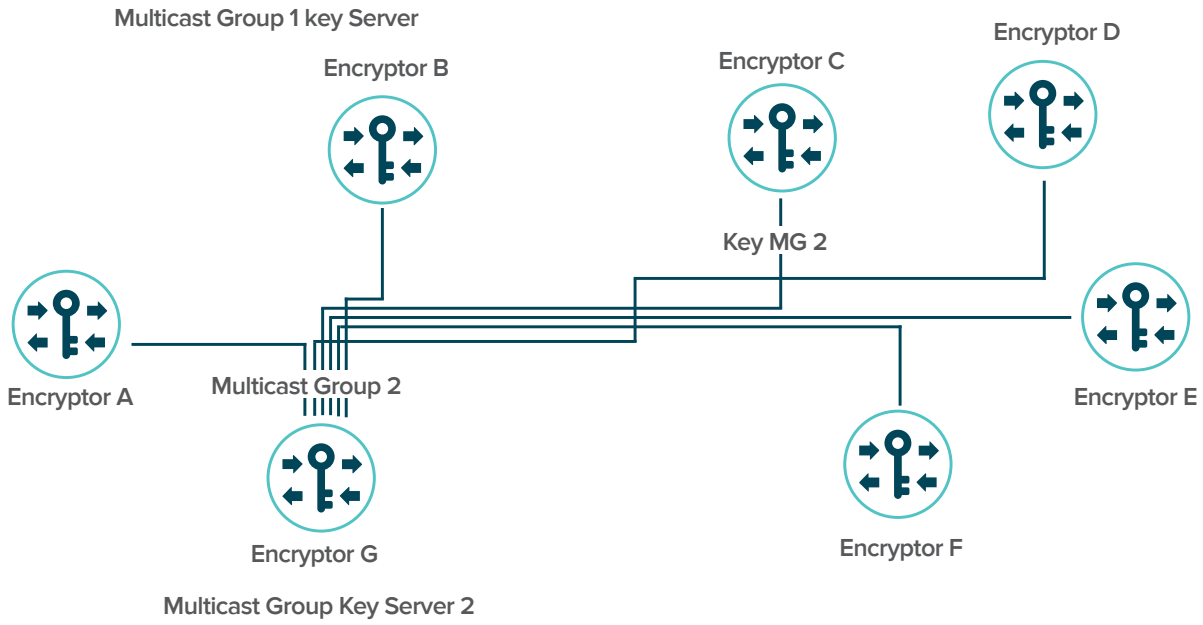
In this scenario, Senetas key management supports the combination of pairwise key system with a distributed group key system. This allows multicast frames to be encrypted with a group key when using a point-to-multipoint topology. For unicast frame encryption, pairwise keys are used; while multicast frames are encrypted using the group key system. As multicast groups can originate at different sites, the encryptor at such sites must be able to act as group key server for the multicast groups originating there.

For unicast frame encryption each encryptor has a table with the local and remote MAC addresses. Security associations are created automatically. The MAC addresses are automatically learned and assigned to the security associations using a proprietary auto-discovery protocol. Multicast groups can either be discovered in discovery mode and be added automatically, or they can be added manually. The key servers work independently of each other and thus offer redundancy. Each multicast group has a senior member that is responsible for the key generation, the key exchange and the key updates. If this senior member drops out, the next member of the multicast group is promoted to senior member and takes over. The group key system ensures that the right keys are available at the right time to the group members. The group key server for that group generates the keys for that group, using a hardware-based true random number generator for the seed.

A multicast group can comprise all sites:



Or it can comprise only a subset of the sites.



Each multicast group has its own key and up to 256 individual multicast groups are supported. Broadcast frames are treated as a “special case” of multicast and are all encrypted using the same broadcast key.

GROUP KEY SYSTEM

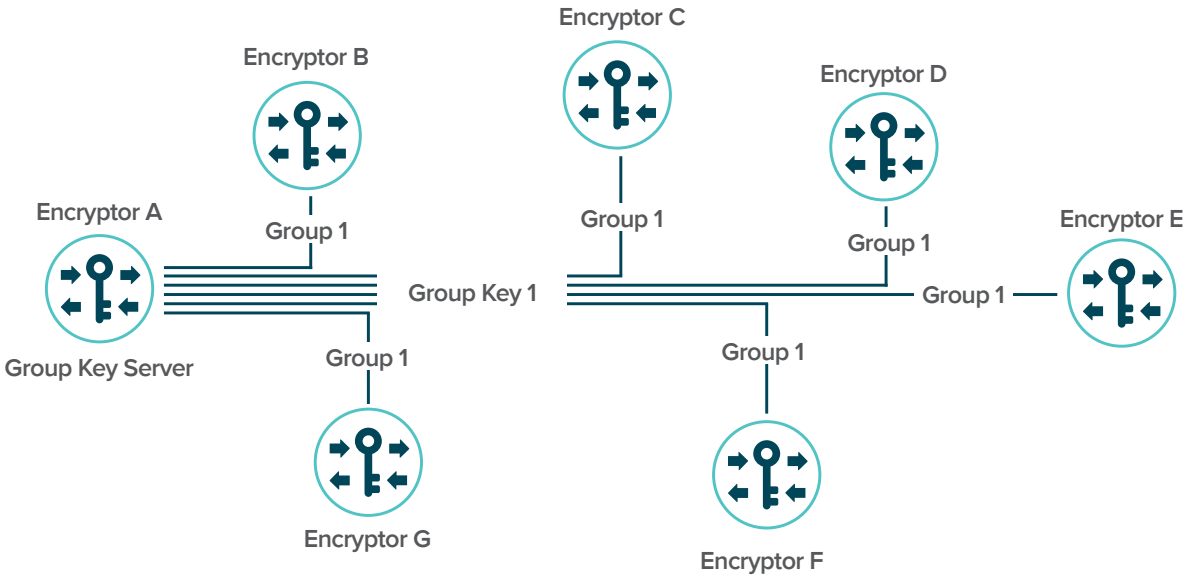
Group keys are based on the principle that for the communication within a defined group the same key is used to encrypt the communication. The membership in one group does not exclude a member from concurrent membership in other groups. For the communication within different groups different keys are used. Keys are unique to a group and separate the groups cryptographically. A group consists of two or more members. For VLAN-based Carrier Ethernet networks, group assignment is based on the VLAN tag. A group can consist of one or multiple VLANs. Each group uses an additional authentication step with each group member having an additional certificate per group. The maximum number of certificates per encryptor is 64. The cryptographic separation of groups combined with support for distributed key servers creates the foundation for a multi-tenancy in which all tenants belong to the same PKI. Group keys work for all three basic topologies.

POINT-TO-POINT (E-LINE)

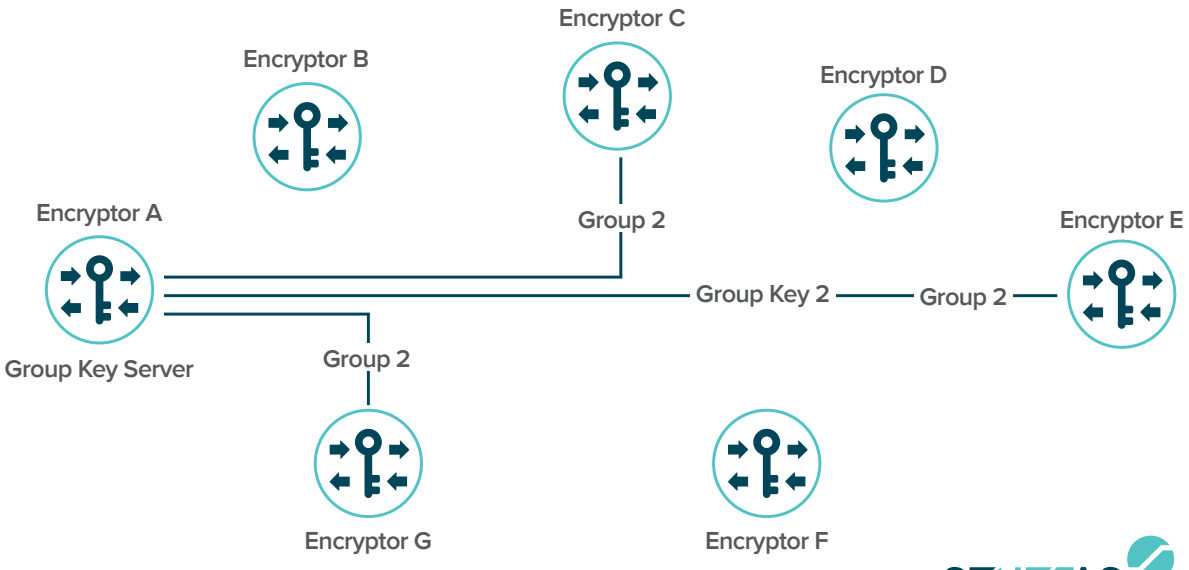
One encryptor is the group key server and generates and distributes the group key to the other group member.

POINT-TO-MULTIPOINT (E-TREE)

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

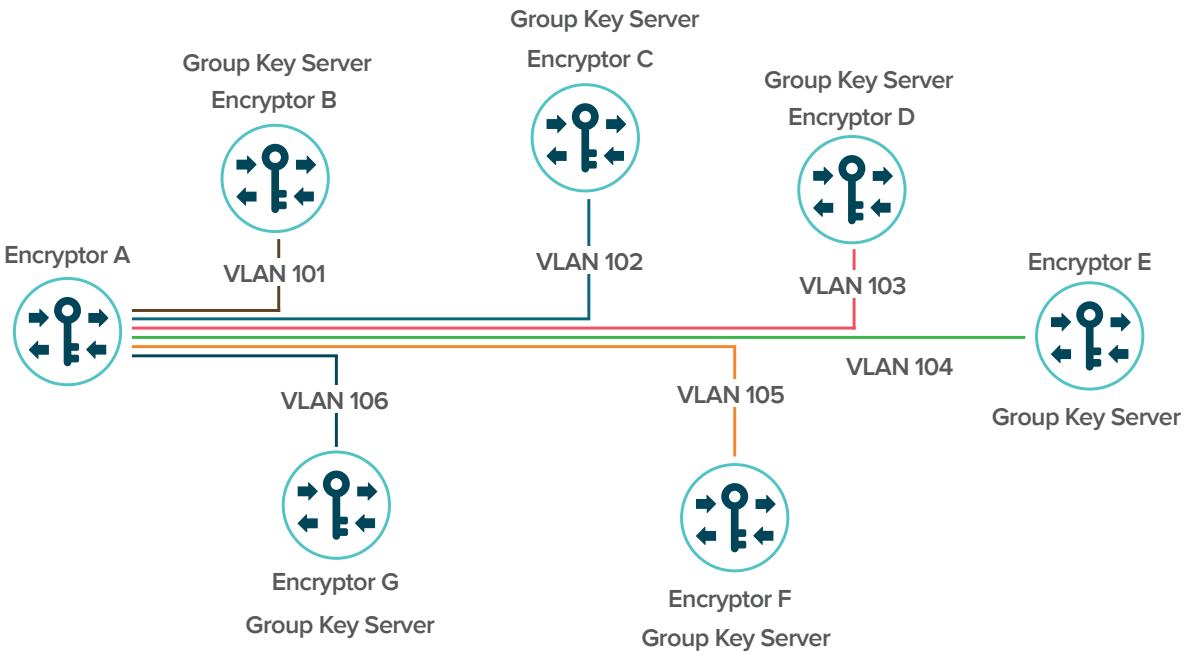


Multiple groups with different memberships can be layered on top of each other:

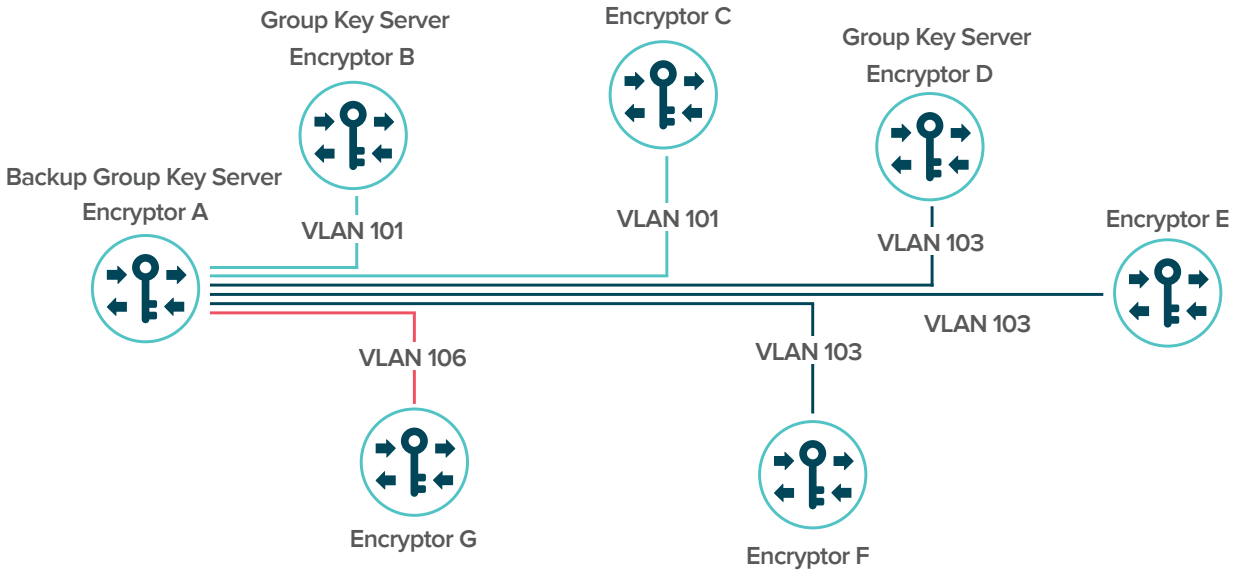


SENETAS
Security without compromise

Each hub-spoke relationship can be treated as an individual group, with the spoke being the group key server:



Or, a mix of VLANs with single or multiple members:

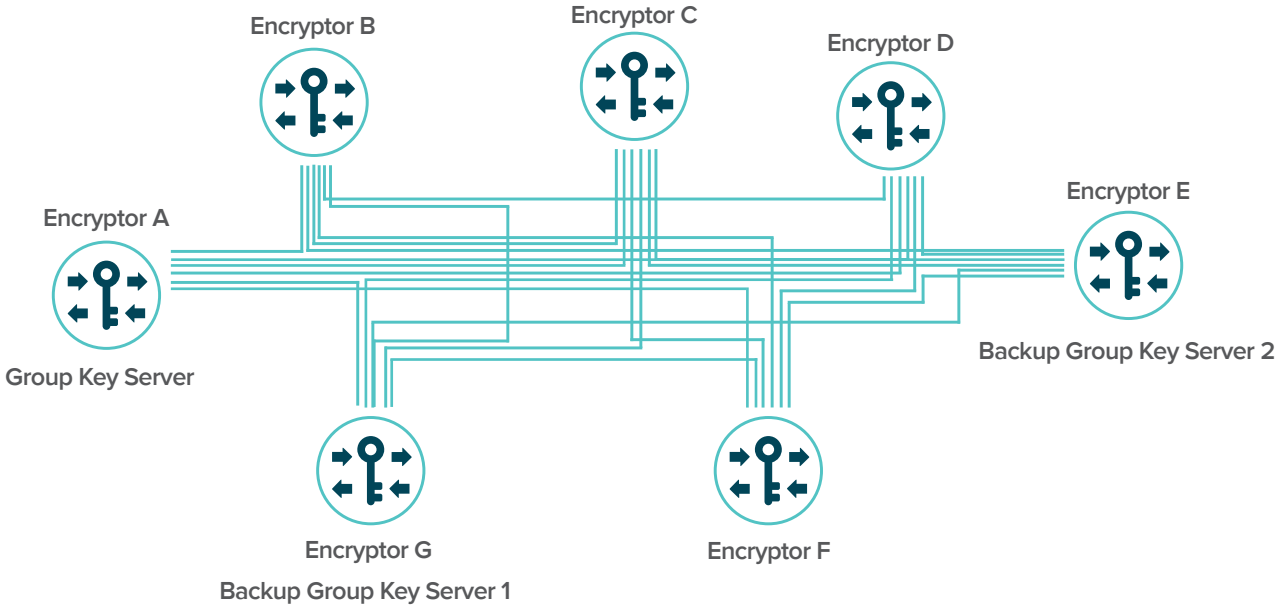


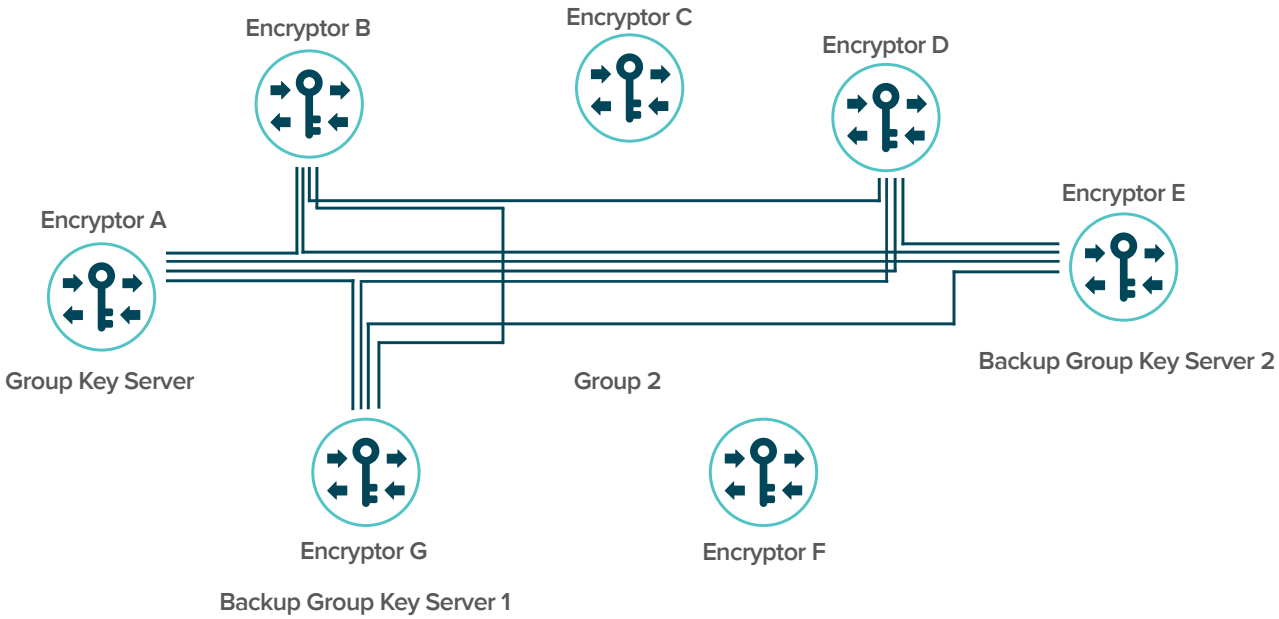
MULTIPOINT-TO-MULTIPOINT

In multipoint-to-multipoint topologies, a group key system allows the layering of different groups. (eg. the individual mambers of a VLAN).

If that VLAN covers all sties, then all sites are members of this group (unless specifically excluded).

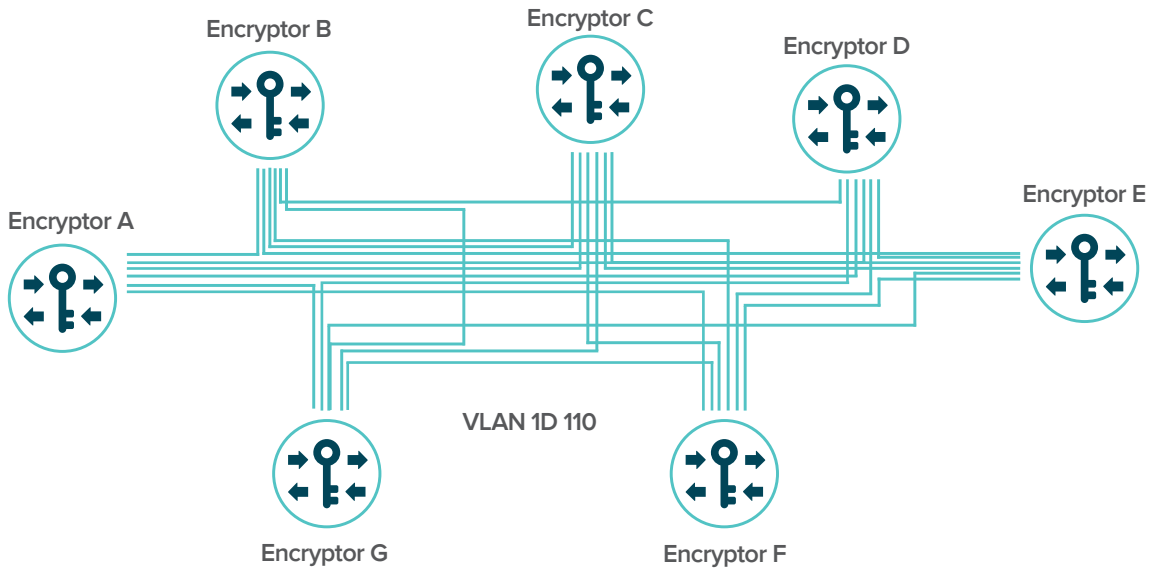
SENETAS
Security without compromise


Encryptor B
Encryptor C
Encryptor D
Encryptor A
Encryptor E
Group Key Server
Backup Group Key Server 2
Encryptor G
Encryptor F
Backup Group Key Server 1

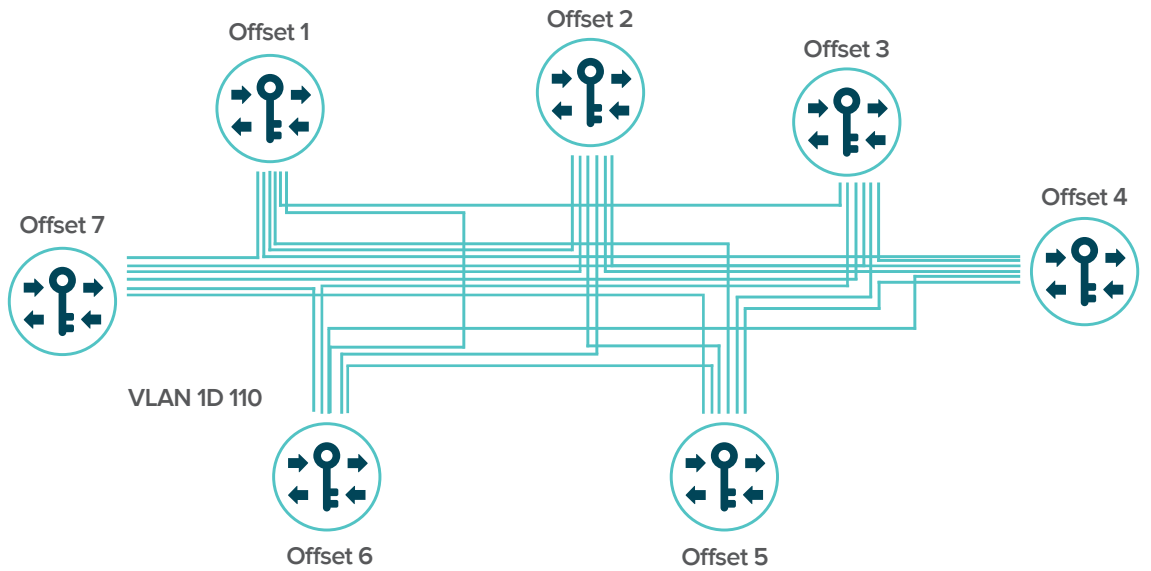

Encryptor B
Encryptor C
Encryptor D
Encryptor A
Encryptor E
Group Key Server
Backup Group Key Server 2
Group 2
Encryptor G
Encryptor F
Backup Group Key Server 1

COUNTER IN GROUP KEY SYSTEMS

Using authenticated encryption, a group shares both the key and the counter. Each group member uses a different counter offset that is transported together with the counter reading in the SecTag of each encrypted frame.



The assignment in terms of counter reading looks as follows:



SENETAS
Security without compromise

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN series encryptors are supported and distributed globally by Gemalto N.V. under its 'SafeNet' encryption brand. Gemalto also provides pre-sales technical support to hundreds of accredited partners globally: systems integrators, networks providers, Cloud and data centre service providers, telecommunications companies and network security specialists.

www.safenet-inc.com/data-encryption/network-encryption/

SENETAS PARTNERS

Senetas works exclusively with leading systems integrators and network service providers across more than 35 countries worldwide.

Our master distributor, Gemalto, and its global network of partners have proven expertise in high-speed data networks and data protection.

What's more, Senetas partners are committed to investing in the latest technical training for network data protection, high-speed data encryption and customer needs analysis.

TALK TO SENETAS OR OUR PARTNERS

Senetas also works with customers' existing data network service providers, systems integrators and information security specialists to specify the optimal high-speed encryption solution for your needs.

The optimal specification of Senetas CN Series encryptors for your network data protection is dependent upon many factors, including IT and network environments, technical and business needs.

Wherever you are, simply contact Senetas to discuss your needs. Or, if you prefer, your service provider may contact Senetas on your behalf.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com