inside-it.ch

PRÄSENTIERT:

LAYER 2-VERSCHLÜSSLER FÜR METRO UND CARRIER ETHERNET

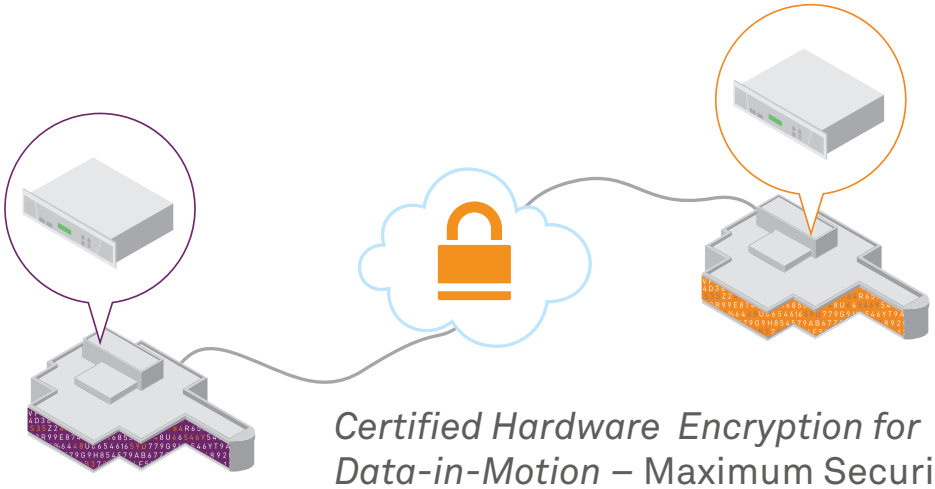
EVALUATIONSHILFE

(KURZFASSUNG)

Version 1.1, 21. Dezember 2014

---

www.uebermeister.com
cjaggi@uebermeister.com



Certified Hardware Encryption for Data-in-Motion – Maximum Security AND Network Performance.
Market Leaders' First Choice!

SafeNet and **Senetas** provide the world's leading **high speed encryption security without compromise.** We deliver **maximum performance, near-zero overhead with "set and forget" simplicity, and low total cost of ownership.**

Whatever your needs – entry level 10Mbps to "carrier-grade" 10Gbps, **we ensure mission-critical protection and performance.** And that's certified!

Your first choice for robust dedicated encryption. Contact SafeNet to protect Intellectual Property, privacy and your reputation from data network breaches. Solutions include time- and bandwidth-sensitive voice and video streams, metadata and traffic monitoring – for enterprise and government organizations.

SafeNet. THE DATA PROTECTION COMPANY
www.safenet-inc.com

SENETAS
Security without compromise
www.senetas.com

Einleitung

Metro und Carrier Ethernet setzt sich immer mehr als bevorzugte Lösung für Metroplitan Area Networks (MAN) und Wide Are Networks (WAN) durch. Einfachheit, Leistungsfähigkeit und tiefere Kosten - kombiniert mit zunehmender Verfügbarkeit und verbesserter Interoperabilität - sind die entscheidenden Faktoren. Metro und Carrier Ethernet verfügen aber über keine eingebaute Sicherheit. Deshalb braucht und gibt es Sicherheitslösungen, welche Ethernet nativ unterstützen: Ethernet-Verschlüssler. Eine Einführung in Ethernet-Verschlüsselung für Metro und Carrier Ethernet ist unter folgender URL verfügbar:

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

Nur native Ethernet-Verschlüssler sind echte Ethernet-Verschlüssler

Nicht alles, was als Ethernet-Verschlüssler vermarktet wird, ist ein nativer Ethernet-Verschlüssler. Transportiert man Ethernet (Layer 2) mittels eines Klimmzugs über IP (Layer 3), so ist Ethernet IP-Nutzlast und kann mittels IPSec verschlüsselt werden. Das ist allerdings ziemlich ineffizient und verringert die Leistung des MANs oder WANs. Um das Ganze noch komplizierter zu machen gibt es mit MACSec einen IEEE-Standard zur Verschlüsselung von lokalen Ethernet-Netzwerken. Für MANs und WANs ist dieser allerdings eher der Kategorie „Unbrauchbar“ zuzuordnen. Schliesslich kommt es kaum jemandem in den Sinn, Pantoffeln als geeignetes Schuhwerk für lange Wanderungen zu bezeichnen. Innerhalb einer Wohnung oder eines Hauses sind sie aber durchaus angebracht. Gleich verhält es sich bei MACSec im Vergleich zu brauchbaren und effizienten Lösungen. Bei MACSec fehlt es an vielem und speziell Schlüsselverwaltung, Verschlüsselungsmodi und die Unterstützung von Verschlüsselungsoffsets genügen den Anforderungen von Metro und Carrrier Ethernet nicht im geringsten. Für Metro und Carrier Ethernet-Netzwerke macht eine Hop-to-Hop-Verschlüsselung schlichtwegs keinen Sinn. Benötigt wird vielmehr eine End-to-End-Verschlüsselung, denn das Ziel ist, die Verbindung zwischen den Standorten komplett abzusichern. Deshalb scheidet MACSec in praktisch allen Fällen von vornherein als Lösung aus. Eine Ausnahme bilden die raren Konstellationen, in denen gilt: Hop = End. Da aber MACSec nur den Transport Modus kennt, bietet es aber auch in solch einem einfachen Szenario deutlich weniger Sicherheit als eine ausgereifte Ethernet-Verschlüsselung,

Die Komplexität der Evaluation

Die Evaluation von Ethernet-Verschlüsslern ist komplex. Netzwerkverschlüssler sind bifunktional: Auf der einen Seite handelt es sich um Sicherheitsgeräte und auf der anderen Seite um Netzwerkgeräte. Ein Ethernet-Verschlüssler ist Verschlüssler und Switch in einem. Entsprechend hoch sind auch die Anforderungen. Vorzugsweise unterstützen sie sowohl die verwendete Netzwerkinfrastruktur als auch den vorgesehenen Verwendungszweck. Entscheidend dafür ist eine Kombination aus Hardware und Software, die eng miteinander verzahnt ist. Es kommt nicht nur darauf an, welche Funktionalität geboten

wird, sondern auch, wie sie implementiert ist. Ein guter Ethernet-Verschlüssler bietet nicht nur Sicherheit für den Datenverkehr, sondern ist auch ein vollwertiges und sicheres Netzwerkgerät. Virtuelle Appliances scheiden deshalb in den meisten Fällen aus.

Unterschiedliche Kunden – unterschiedliche Anforderungen

Unterschiedliche Kunden haben unterschiedliche Anforderungen. Ein Ethernet-Verschlüssler kann für einen Teil der Kunden sämtliche vorhandenen und absehbaren Anforderungen erfüllen, während er die Anforderungen anderer Kunden nicht abzudecken vermag. Insofern gibt es nicht den besten Ethernet-Verschlüssler, sondern nur Ethernet-Verschlüssler, welche unterschiedliche Anforderungen abdecken. Diese Anforderungen betreffen einerseits die Netzwerkunterstützung und Netzwerkfunktionalität und andererseits die Sicherheit. Es gibt z.B. erstaunlicherweise auch heute noch Kunden, bei denen authentisierte Verschlüsselung im Anforderungsprofil fehlt. Falls jemand wirklich darauf verzichten möchte, so ist das definitiv die Ausnahme und nicht die Regel. Für Dienstleister, die Verschlüsselung als Managed Service anbieten, sieht die Sachlage allerdings anders aus. Der Grund dafür liegt in den unterschiedlichen Kunden mit unterschiedlichen Anforderungen. Für Anbieter von Managed Encryption und Managed Security ist die Auswahl entsprechend eingeschränkt.

Inhaltsverzeichnis

Rechenzentren und Standorte abhörsicher vernetzen

Verschlüsselung und IT-Sicherheit
Made in Germany

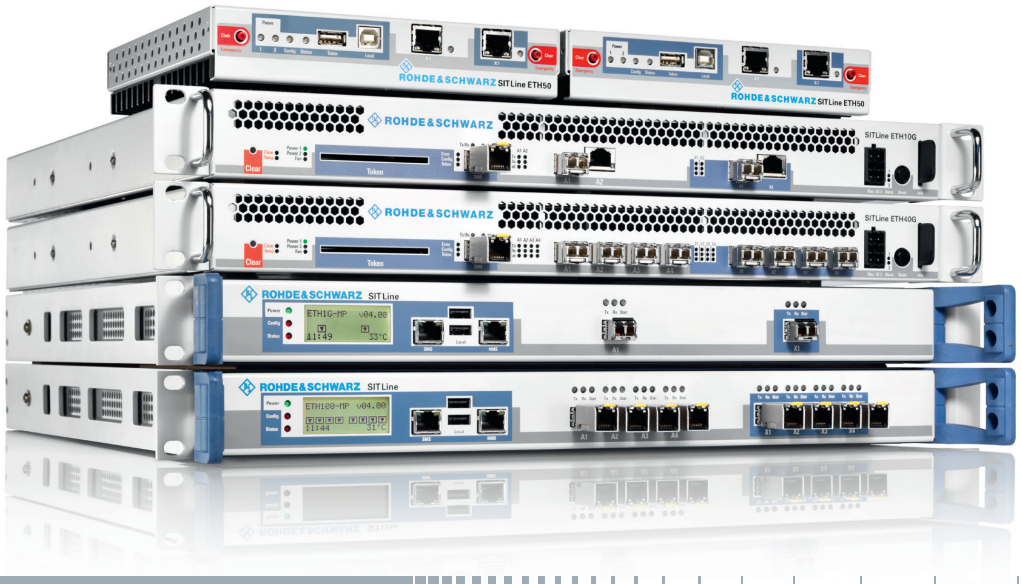
Bei der Vernetzung von Standorten und Rechenzentren verlassen sensible Daten die geschützte IT-Infrastruktur. Doch optische und elektrische Leitungen können einfach abgehört werden.

R&S®SITLine ETH verschlüsselt die Daten vor der Übertragung – kostengünstig, hochverfügbar, BSI-zugelassen.

- Ethernet-Verschlüsseler mit bis zu 40 Gbit/s Datendurchsatz pro Gerät
- Sichere Datenübertragung über Festnetz, Richtfunk und Satellit
- Minimale Latenz für den Einsatz (3µs) in Echtzeit-Umgebungen
- BSI-zugelassen bis VS-NfD und NATO RESTRICTED

Fordern Sie unverbindlich weitere Informationen an oder vereinbaren Sie gleich einen individuellen Termin mit unseren Experten unter:
Tel.: 030 / 65884-223
info.sit@rohde-schwarz.com

www.rohde-schwarz.com/sitline



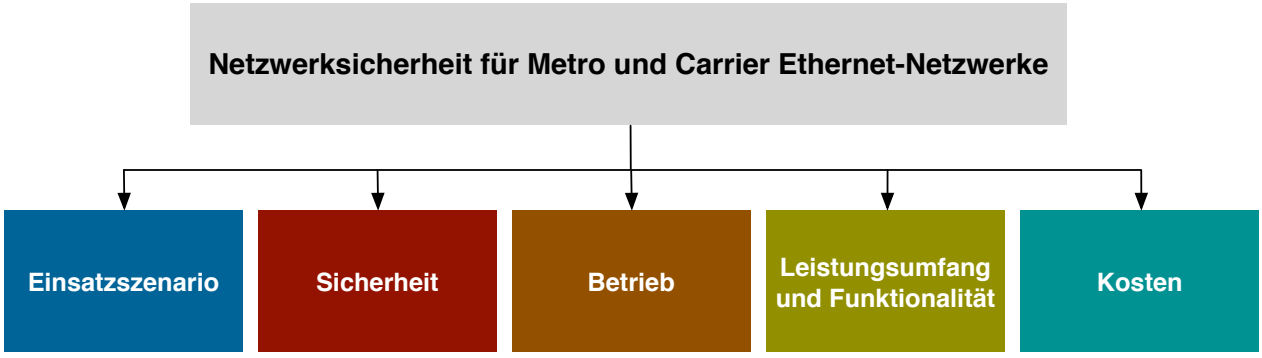
ROHDE&SCHWARZ

Sektion 1: Vorgehensweise

Mit Carrier Ethernet lassen sich Standorte einfach und kosteneffizient vernetzen: Lokal, regional und überregional. Nur sicher sollte es sein. Das gilt sowohl für die übertragenen Daten wie auch für das Netzwerk. Keiner soll ungesicherte Nutzdaten abgreifen können. Ebenfalls unerwünscht ist das Einschleusen unauthorisierter Daten in das Netzwerk. Verhindert wird das mit einer Kombination von Netzwerkverschlüsselung, Intrusion Detection, Intrusion Prevention und Firewall. Bei Verwendung von authentisierter Verschlüsselung auf Layer 2 ist ein solcher Gesamtschutz durch den Einsatz von AES-GCM möglich.

Es gibt viele Produkte, die als Ethernet-Verschlüssler angeboten werden, denn Ethernet lässt sich auf unterschiedliche Weise verschlüsseln. Die gebotene Sicherheit und Netzwerkkompatibilität variieren hingegen stark. Die beste Lösung bietet immer ein Produkt, das maximale Netzwerkkompatibilität mit optimaler Sicherheit in Bezug auf das Netzwerk verbindet, und das zu vernünftigen Kosten.

Wie findet man nun die geeignete Lösung? Ausgangspunkt ist das Einsatzszenario. Es wird einerseits durch das vorhandene und geplante Firmennetzwerk und andererseits durch die Transportnetzwerke bestimmt. Anschliessend legt man die gewünschte Sicherheit und die betrieblichen Anforderungen fest. So lässt sich der benötigte Leistungsumfang definieren. Dieser wiederum ist die Grundlage zur Auswahl geeigneter Produkte. Abschliessender Faktor sind die Anschaffungs- und Betriebskosten der geeigneten Produkte. Der Vorgang besteht also aus dem Festlegen des Anforderungsprofils, dem Finden geeigneter Produkte und der Wahl der effizientesten Lösung.

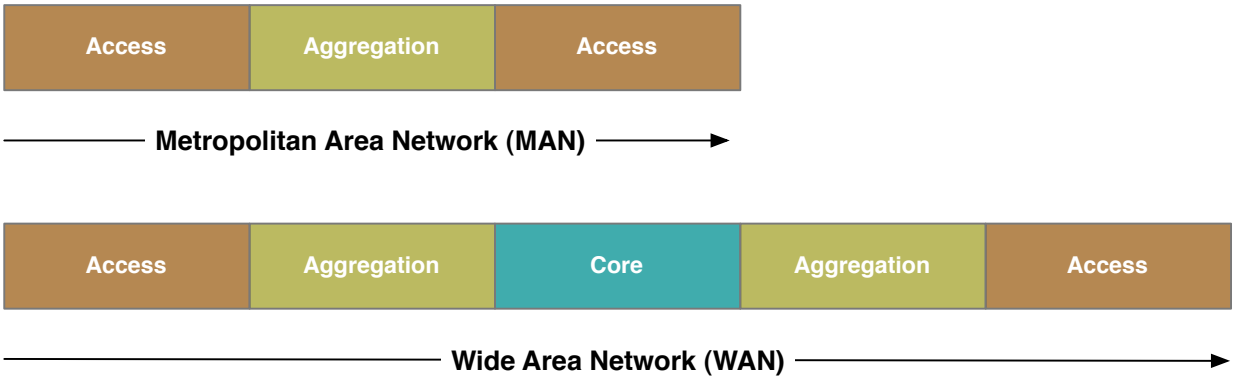


Sektion 2: Einsatzszenario

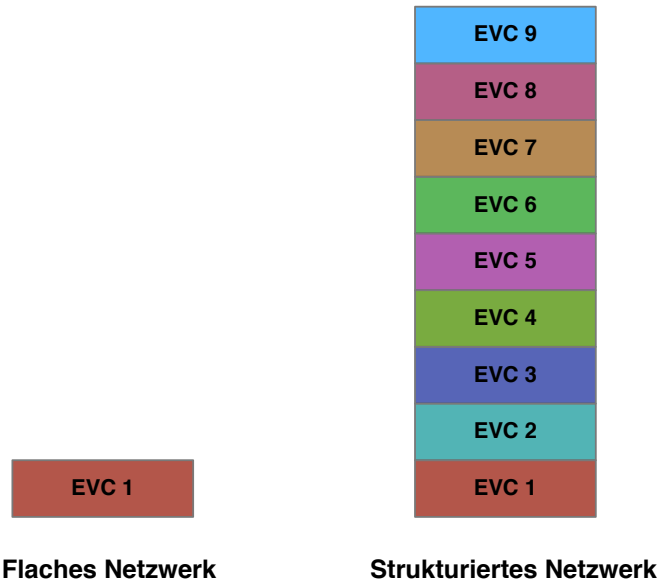
Zur Ermittlung des Anforderungsprofils fängt man am besten mit dem Einsatzszenario des MANs oder WANs an. So lässt sich der benötigte Leistungsumfang des Verschlüsslers definieren.

1. MAN oder WAN?

Carrier Ethernet im MAN-Bereich unterscheidet sich meist von Carrier Ethernet im WAN-Bereich. Ein MAN stellt teilweise geringere Anforderungen an den Leistungsumfang eines Verschlüsslers als ein WAN.



Mittels VLANs und Ethernet Virtual Channels lassen sich Carrier Ethernet-Netzwerke strukturieren.



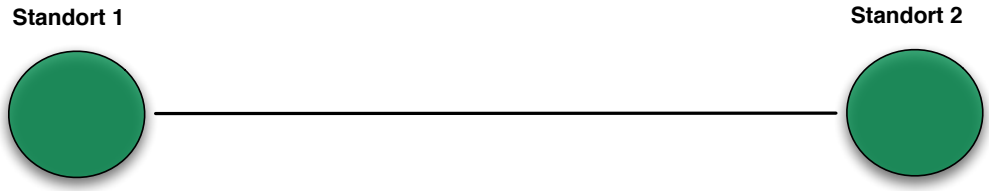
Ein Ethernet Virtual Channel (EVC) entspricht dabei einem Ethernet-Netzwerk, das

wiederum mehrere VLANs beinhalten kann. In vielen Fällen ist es aber vorteilhaft oder gar notwenig, mehrere Ethernet Virtual Channels zu verwenden. So lässt sich das Netz besser strukturieren und segmentieren. SLAs beziehen sich regelmässig auf EVCs. Bei Verwendung mehrerer EVCs lassen sich je nach Anforderung unterschiedliche SLAs wählen. So kann das Kostenprofil pro EVC optimiert werden.

2. Netzwerktopologien und Einsatzszenario

2.1. Punkt-zu-Punkt

Will man nur zwei Standorte verbinden, so ist das relativ einfach, denn Punkt-zu-Punkt-Verbindungen sind am einfachsten abzusichern. Aufgrund der homogenen Verbindung sind die Anforderung an den Funktionsumfang im Vergleich zu den anderen Topologien relativ bescheiden.

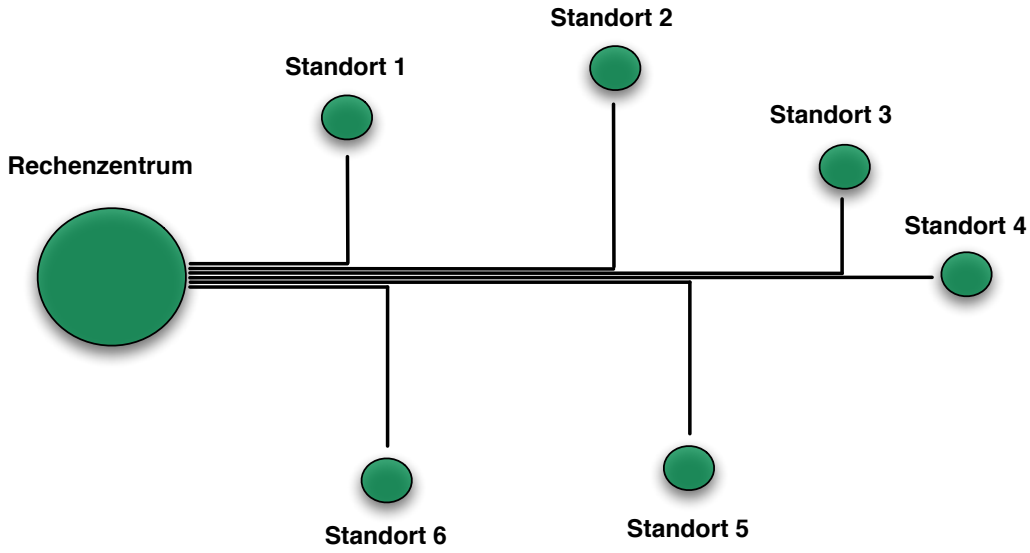


Bei der Netzwerksicherheit ist es wie in vielen anderen Bereichen. Es stellt sich die Frage, ob man sie selbst betreibt oder ob der Betrieb an einen spezialisierten Anbieter ausgelagert werden soll. Für letzteres muss die Sicherheitslösung mandantenfähig sein, wobei die Schlüsselhoheit und Verschlüsselungshoheit immer beim Mandanten liegen muss. Liegt die Schlüsselhoheit beim Dienstleister, so hat dieser die Verfügungsgewalt über die Schlüssel. Gleiches gilt für die Verschlüsselungshoheit. Wenn der Dienstleister über diese verfügt, so kann er die Verschlüsselungsfunktion ausschalten und die Sicherheit ist für den Mandanten nicht mehr gewährleistet.

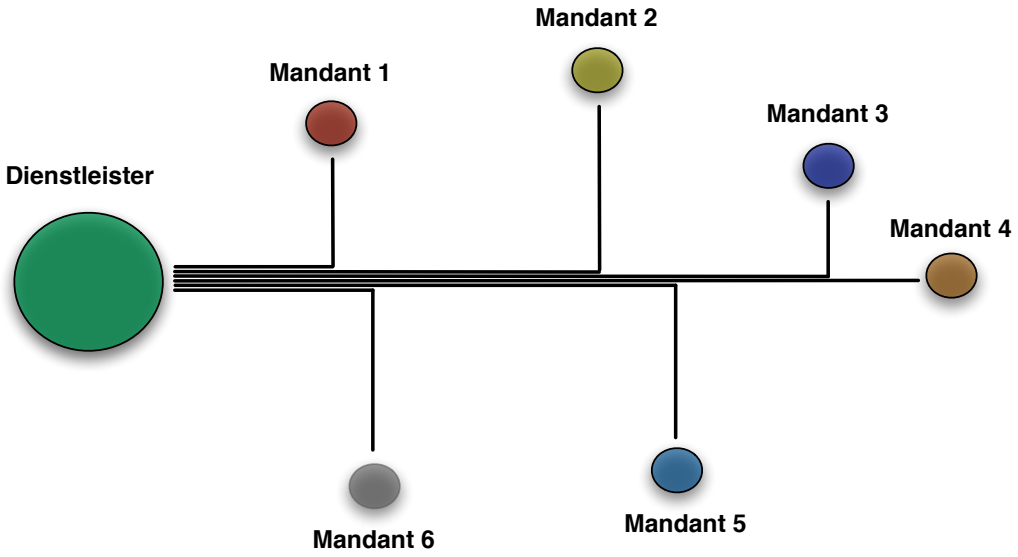
2.2. Punkt-zu-Multipunkt

Die Verbindung mehrerer Standorte mit einer Zentrale wird oft mittels einer Punkt-zu-Multipunkt-Topologie hergestellt. Dabei handelt es sich um mehrere Punkt-zu-Punkt-Verbindungen, die von einem zentralen Punkt aus gehen. Im Vergleich zu einzelnen Punkt-zu-Punkt-Verbindungen senkt das die Kosten und erhöht die möglichen Einsatzszenarien, bringt aber entsprechend mehr Komplexität.

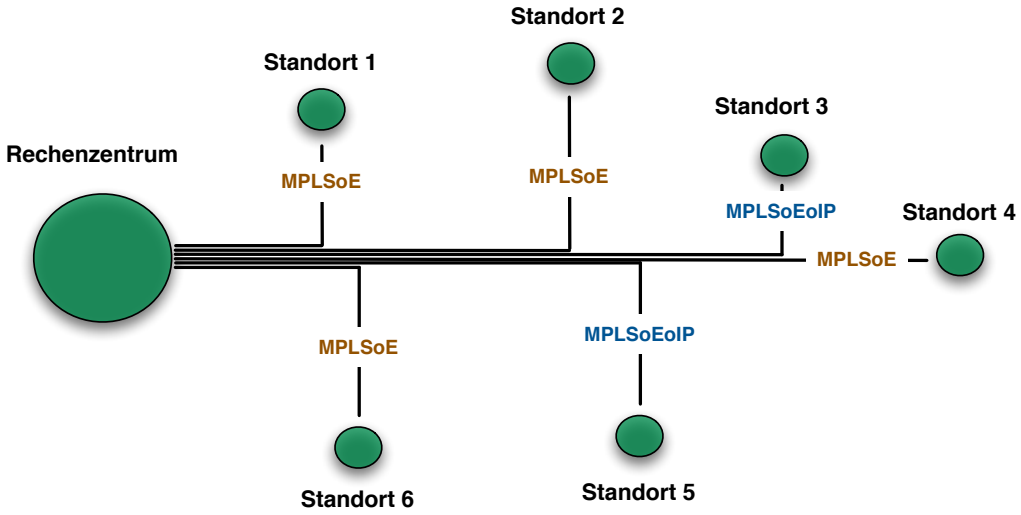
Wird die Netzwerksicherheit innerbetrieblich selbst gewährleistet oder an einen Dienstleister ausgelagert, so gelten die gleichen Voraussetzungen in Bezug auf Mandantenfähigkeit wie bei den Punkt-zu-Punkt-Verbindungen.



Anders sieht es aus, wenn mehrere Mandanten bedient werden.

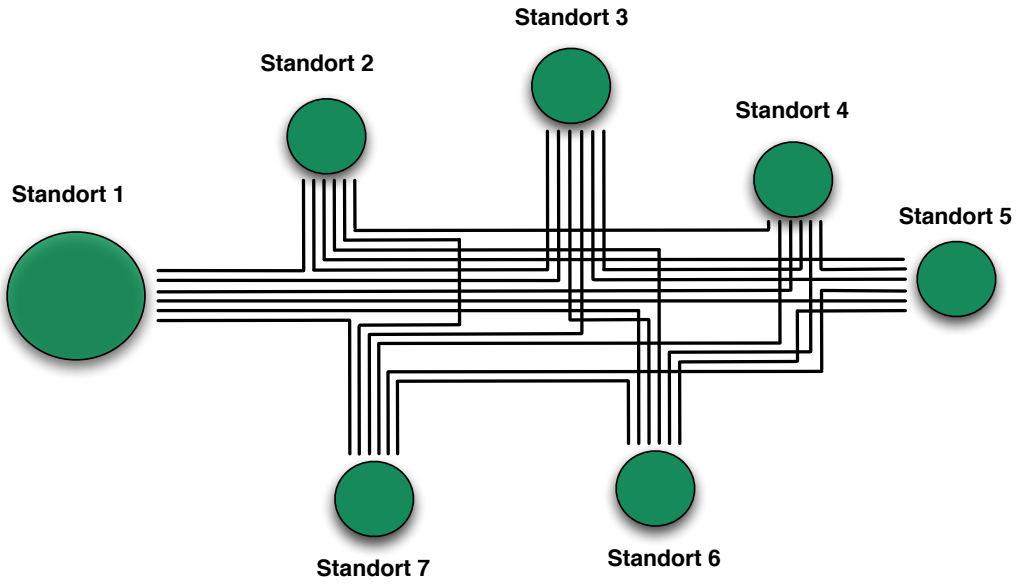


Einfache Mandantenfähigkeit genügt hier nicht mehr. Vielmehr ist Mehrmandantenfähigkeit gefragt. Für jeden Mandanten braucht es eine eigene Schlüssel- und Verschlüsselungshoheit.
Bei Punkt-zu-Multipunkt-Topologien kann es durchaus auch vorkommen, dass nicht alle Standorte über Carrier Ethernet angebunden sind. Ein Szenario sind MPLS-Netzwerke,bei denen ein Grossteil der Standorte mittels Carrier Ethernet verbunden ist (MPLSoE), ein kleiner Teil aber nur über IP erreichbar ist. In diesem Fall ist es von Vorteil, wenn ein Verschlüssler auch Ethernet over IP (EoIP) unterstützt und so MPLSoE auch mit diesen Standorten abgesichert werden kann.



2.3. Multipunkt-zu-Multipunkt

Bei einer Multipunkt-zu-Multipunkt-Topologie sind im Gegensatz zu einer Punkt-zu-Punkt-Topologie alle Standorte direkt miteinander verbunden. Es gibt keinen zentralen Standort mehr. Jeder Standort kann dasselbe wie der zentrale Standort bei einer Punkt-zu-Multipunkt-Topologie: An alle Standorte Frames senden und von allen Standorten Frames empfangen. Mittels VLANs und EVCs lassen sich solche Multipunktnetze strukturieren und segmentieren.



Ein mandantenfähiger Betrieb solcher Netzwerke und deren Sicherheit ist in der Regel durchaus möglich. Problematischer ist es in Bezug auf die Mehrmandantenfähigkeit, welche zur Zeit nur mit grossen Abstrichen realisierbar ist. Voraussetzung dafür wäre eine komplette Virtualisierung der Verschlüssler, inklusive der Device ID. Hardware lässt sich nur bis zu einem bestimmten Grad so virtualisieren, dass die Sicherheit und der Betrieb nicht darunter leiden.

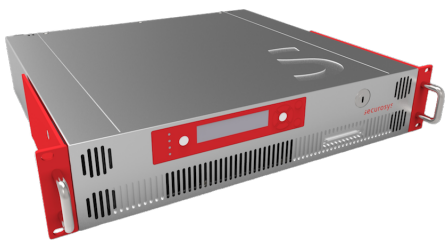
Auch bei Multipunkt-Netzwerken kann es insbesondere bei MPLS-Netzwerken vorkommen, dass ein beteiligter Standort nur über IP eingebunden werden kann. Eine Lösung bedingt deshalb die Unterstützung von Ethernet over IP (EoIP).

Die wichtigsten Fragen:

- Wie sieht die Topologie des zu schützenden Netzwerks aus?
- Handelt es sich um ein MAN oder ein WAN?
- Ist eine Erweiterung des zu schützenden Netzwerks absehbar und falls ja, hat das Auswirkungen auf die Netzwerktopologie?
- Welche Transportnetzwerke müssen an den Standorten unterstützt werden: Nur Ethernet oder Ethernet und IP?
- Wird die Sicherheit des Netzwerkes selbst betrieben oder ist sie ausgelagert?
- Wird Netzwerksicherheit als Dienstleistung für Mandanten angeboten? Falls ja, sind es mehrere Mandaten pro Netzwerk?

securosys
SWISS SECURITY TECHNOLOGIES
FOR COMMUNICATIONS SYSTEMS

Secure Your Communications - Trust Your Equipment



Securosys is your source for highest security, trusted communications equipment:

- Layer-2 Encryptors: 1Gb - 10Gb +
- VPN Server, Clients, Bridge
- Hardware Security Modules (HSM)

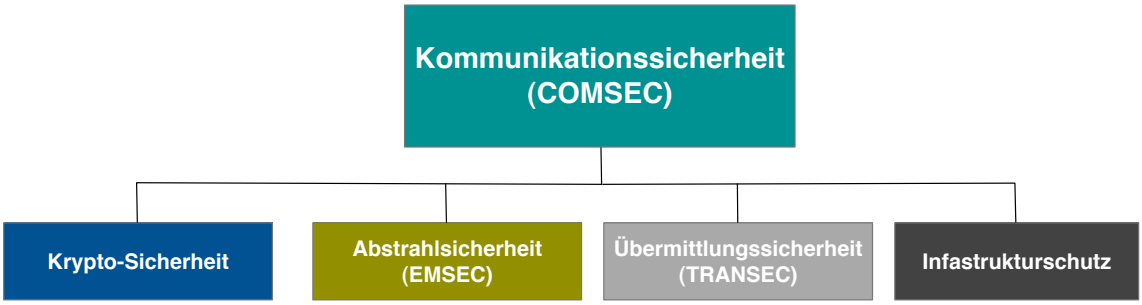
Our products are designed and manufactured in Switzerland **free of contaminating influences** and **without backdoors** to exploit.

Contact us for a trustworthy solution matching your requirements:
+41 44 552 31 00 info@securosys.ch www.securosys.ch

SWISS MADE

Sektion 3: Sicherheit

Kommunikationssicherheit besteht aus mehreren Bereichen, die in ihrer Gesamtheit als COMSEC bezeichnet werden.

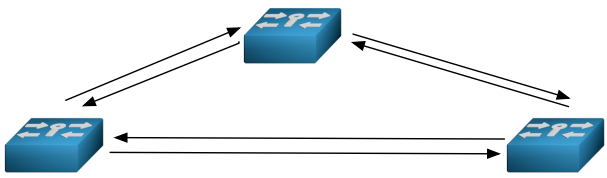


Die meisten dieser Bereiche setzen Hardware-Eigenschaften voraus. Ohne Hardware ist volle Kommunikationssicherheit nicht möglich.

1. Krypto-Sicherheit

Oberflächlich gesehen besteht die Krypto-Sicherheit vorwiegend aus einer Blockchiffre, einem Betriebsmodus und Schlüsseln. Bei aktuellen Ethernet-Verschlüsslern gebräuchlich sind AES als Blockchiffre, GCM als Betriebsmodus und 256-Bit als Schlüssellänge. Taucht man ein bisschen tiefer, so zeigt sich, dass die Krypto-Sicherheit äusserst komplex ist. Die Schlüsselverwaltung ist mehrschichtig und setzt voraus, dass auf den Verschlüsslern ein Anfangsgeheimnis vorhanden ist. Die erste Schwierigkeit besteht darin, das Anfangsgeheimnis sicher auf die sichere Hardware zu bekommen. Für eine Kommunikation braucht es aber mehr als eine Partei. Die beteiligten Verschlüssler müssen sich deshalb gegenseitig authentisieren. Ist dies erfolgt, so besteht zwischen den beteiligten Verschlüsslern jeweils eine Connectivity Association. Das heisst, dass die Geräte miteinander verbunden sind und eine Security Association etablieren dürfen.

Connectivity Association

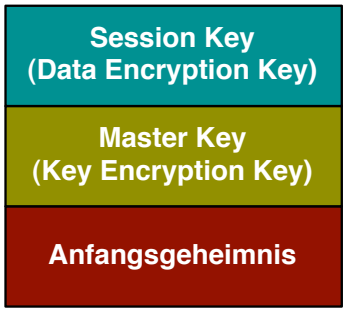


Geräte dürfen miteinander kommunizieren

Authentisierung via Certificate oder Pre-shared Secret/Pre-shared Key

1.1. Die Schlüsselverwaltung

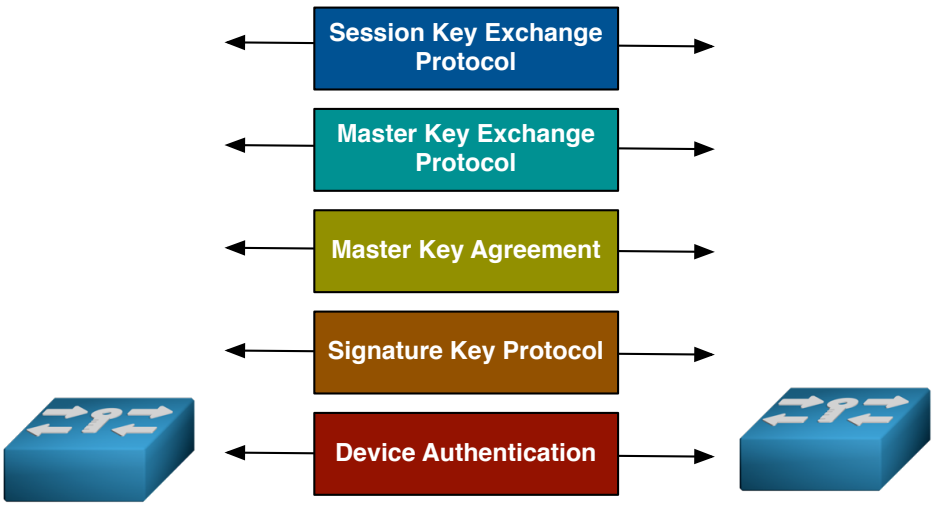
Simplifiziert dargestellt braucht es für die Verschlüsselung ein Anfangsgeheimnis zur Authentisierung, einen Master Key (Key Encryption Key) zum Verschlüsseln des Session Key (Data Encryption Key) und einen Session Key zum Verschlüsseln der Daten.



1.1.1. Anfangsgeheimnisse und Schlüsselhierarchie

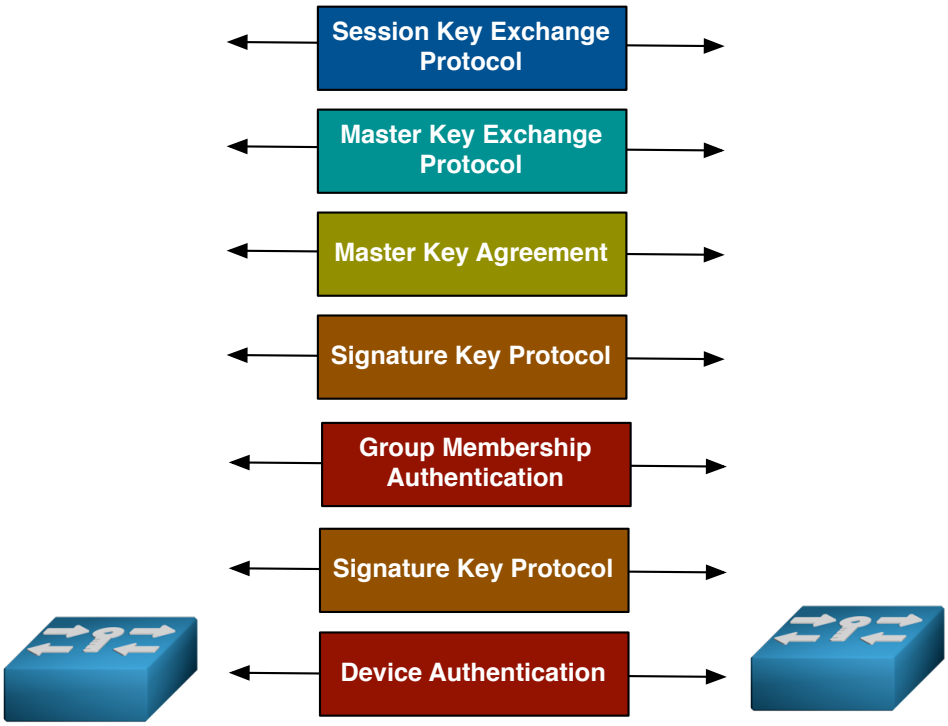
Es ist aber viel komplexer. Zuerst muss etabliert werden, wer mit wem kommunizieren darf. Ist die Connectivity Association erstellt, so braucht es zusätzlich eine Security Association, die festlegt, wie die beiden Beteiligten sicher miteinander kommunizieren. Dafür wird ein Anfangsgeheimnis benötigt. Dabei kann es sich um einen Pre-Shared-Key oder ein Zertifikat handeln. Bei Verwendung von elliptischen Kurven gehört auch die Kurven-Domain dazu.

Vom Anfangsgeheimnis bis zum Session Key laufen mehrere komplexe Prozesse ab, die sowohl in sich selber wie auch in der Abfolge sicher sein müssen.



Noch eine Stufe komplexer ist es bei der Verwendung von Gruppenschlüsselsystemen, da

nicht nur das Gerät sondern auch die Gruppenmitgliedschaft authentisiert werden muss. Dafür braucht es ein zusätzliches gruppenspezifisches Anfangsgeheimnis.



Bei Gruppenschlüsselsystemen ist darauf zu achten, dass nebst der Geräteauthentisierung und der entsprechenden Connectivity und Security Association zusätzlich pro Gruppe eine zusätzliche Connectivity und Security Association besteht.

Für die Generierung von sicheren Schlüsseln braucht es wirklich zufällige Zufallszahlen und für das braucht es Hardware: Einen echten Zufallszahlengenerator. Zudem müssen generierte Schlüssel auf ihre Stärke geprüft werden bevor sie zum Einsatz kommen. Auch für die sichere Aufbewahrung von Schlüsseln geht es nicht ohne entsprechende Hardware. Diese sollte manipulationsresistent sein.

1.1.2. Schlüssel und Schlüsselaustausch

Für den Schlüsselaustausch kommen sowohl symmetrische wie auch asymmetrische Verfahren In Frage. Der Einsatz eines asymmetrischen Verfahrens erfordert deutlich mehr Rechenleistung, gilt aber dafür entsprechend auch als viel sicherer. Eine entscheidende Verbesserung der Sicherheit bietet die Kombination von asymmetrischen und symmetrischen Verfahren, wie z.B. die Kombination von Diffie-Hellman mit symmetrischer Überschlüsselung der Teilschlüssel.

Bei einer symmetrischen Vorgehensweise sind alle Schlüssel direkt voneinander abgeleitet. Zuerst wird beim Verschlüssler ein Pre-Shared-Secret eingegeben. Der Master-Key wird intern im Verschlüssler erzeugt und mit dem Shared-Secret verschlüsselt. Der Session-

Key wird ebenfalls vom Verschlüssler erstellt und mit dem Master-Key verschlüsselt. Master- und Session-Key werden jeweils in der verschlüsselten Form über die Leitung zum anderen Verschlüssler übertragen. Anstelle eines Schlüssels können auch nur die zur Berechnung des Schlüssels notwendigen Variablen wie z.B. die Zufallszahl übertragen werden. Das grosse Problem bei dieser Vorgehensweise liegt darin, dass wenn das Shared-Secret irgendwann bekannt wird, jede früher aufgezeichnete Kommunikation entschlüsselt werden kann.

Bei einer asymmetrischen Vorgehensweise werden die Teilschlüssel vollständig im Verschlüssler generiert, ohne dass der Benutzer einen Zugriff darauf hätte. Aus den jeweils ausgetauschten Teilschlüsseln berechnen beide Seiten jeweils das gleiche Shared-Secret. Im Gegensatz zu einem symmetrischen Verfahren kennt hier niemand das Shared-Secret. Der Verschlüssler erzeugt anschliessend intern den Master-Key und verschlüsselt ihn mit dem Shared-Secret. Auch der Session-Key wird vom Verschlüssler erstellt, als Schlüssel dient der Master-Key. Die Übertragung der Master- und der Session-Keys von einem Verschlüssler zum andern erfolgt immer in verschlüsselter Form.
Als asymmetrische Verfahren werden primär Diffie-Hellman und RSA eingesetzt. Diffie-Hellman verwendet in der Standardvariante das so genannte „diskrete Logarithmus Problem“. Dieses Verfahren erzeugt aber bei entsprechender Sicherheit sehr lange Teilschlüssel. Moderne Systeme tendieren deshalb zur Verwendung von Diffie-Hellman mit Elliptic Curve Crypto System (ECC). Dies bietet bei wesentlich kürzeren Teilschlüsseln eine höhere Sicherheit bietet und gilt heute als Standard. Es ist aber dabei zu beachten, dass nicht alle Kurven gleich sicher sind. So gelten z.B. die NIST-Kurven nicht als empfehlenswert. Die Wahl der Kurven respektive der verwendeten Kurven-Standards sollte beim Anwender liegen. Dies bedingt, dass ein Verschlüssler diese Wahl auch zulässt.
Asymmetrische Verfahren unterschreiben die ausgetauschten Teilschlüssel um sicherzustellen, dass sie auch von der richtigen Gegenstelle stammen. Dies kann entweder durch Zertifikate (X.509) kombiniert mit entsprechenden Verfahren (RSA, DAS oder ECC) oder durch Verschlüsselung des Teilschlüssels mit einem Pre-Shared Secret erfolgen.

Die meisten Verschlüssler verwenden eine hybride Herangehensweise, bei der eine Kombination aus asymmetrischer und symmetrischer Verschlüsselung zu Einsatz kommt. Der Datenverkehr wird dabei symmetrisch verschlüsselt.

1.1.3 Austauschfrequenz

Je häufiger der verwendete Session-Key geändert wird, desto geringer ist die Wahrscheinlichkeit, dass er geknackt wird. Die Sicherheit des Schlüssels hängt dabei nicht nur von der Vertraulichkeit, sondern auch von den verwendeten Verfahren und den gewählten Parametern ab. So spielen die Länge des Counters und des ICV eine Rolle. Im GCM-Modus muss z.B. der Schlüssel gewechselt werden bevor sich die Counter wiederholen. Es ist deshalb unerlässlich, dass der Session Key vom System automatisch nach einer bestimmten Anzahl Minuten gewechselt wird.
Das gleiche gilt für den Key Encryption Key (Master Key), der für die Verschlüsselung des Session Keys verwendet wird. Da dieser weniger Daten verschlüsselt, ist die Wechselfrequenz entsprechend tiefer. Auch dieser Schlüssel sollte automatisch ausgewechselt

werden können.

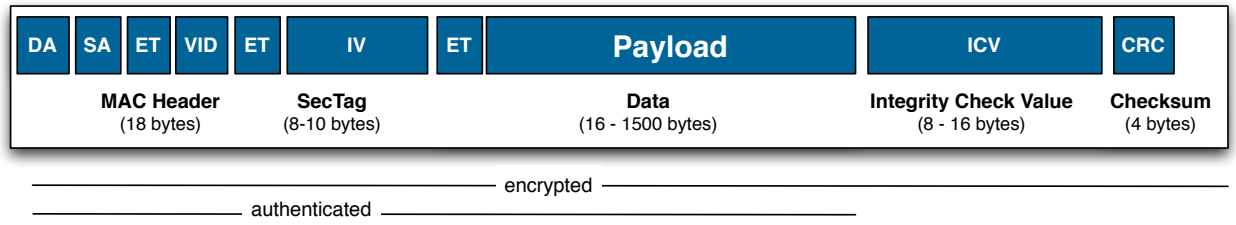
Schlüsseltyp	Wechselfrequenz
Session Key (Data Encryption Key)	alle 1 - 60 Minuten
Master Key (Key Encryption Key)	alle 1 -24 Stunden
Anfangsgeheimnis	alle 12 - 24 Monate

Ein weiterer Aspekt der Schlüsselverwaltung ist die Schlüsselzuweisung. Bei Ethernet kann die entweder port- oder VLAN-bezogen sein. VLANs sind Gruppen, weshalb dazu ein Gruppenschlüsselsystem benötigt wird.

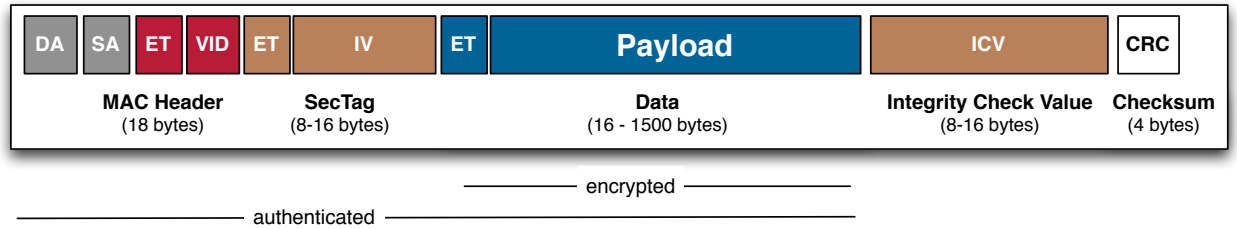
1.2. Der Verschlüsselungsmodus

Für Ethernet gibt es drei unterschiedliche Verschlüsselungsmodi: Frame, Transport und Tunnel. Jeder dieser Modi existiert in authentisierter und unauthentisierter Form. Die Wahl des Modus hängt vom Netzwerk und von den Sicherheitserfordernissen ab. Unauthentisierte Verschlüsselung kann nur die Vertraulichkeit der Daten gewährleisten, ist aber nicht geeignet zum Schutz des Netzwerks, da die Funktionalität der Intrusion Detection, Intrusion Prevention und der Firewall wegfällt, welche bei authentisierter Verschlüsselung vorhanden ist. Eine Lösung mit authentisierter Verschlüsselung ist deshalb aufgrund der höheren Sicherheit einer Lösung ohne authentisierte Verschlüsselung vorzuziehen.

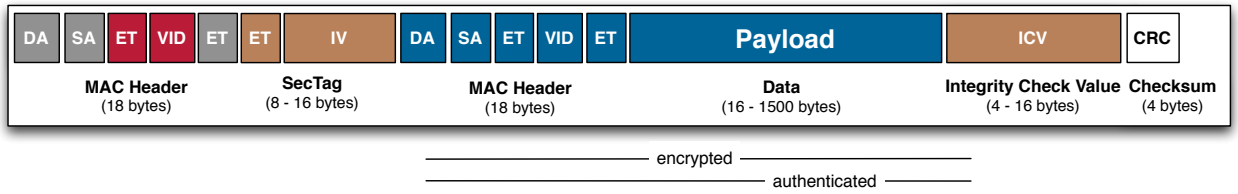
Der Frame-Modus verschlüsselt den ganzen Frame, funktioniert aber nur bei einer direkten Verbindung zwischen den beiden Verschlüsslern.



Der Transport-Modus ist mit sämtlichen Carrier Ethernet-Netzwerken kompatibel.



Der Tunnel-Modus wird bei erhöhten Sicherheitsanforderungen verwendet. Sichtbar sind nur noch die MAC-Adressen der beiden Verschlüssler.

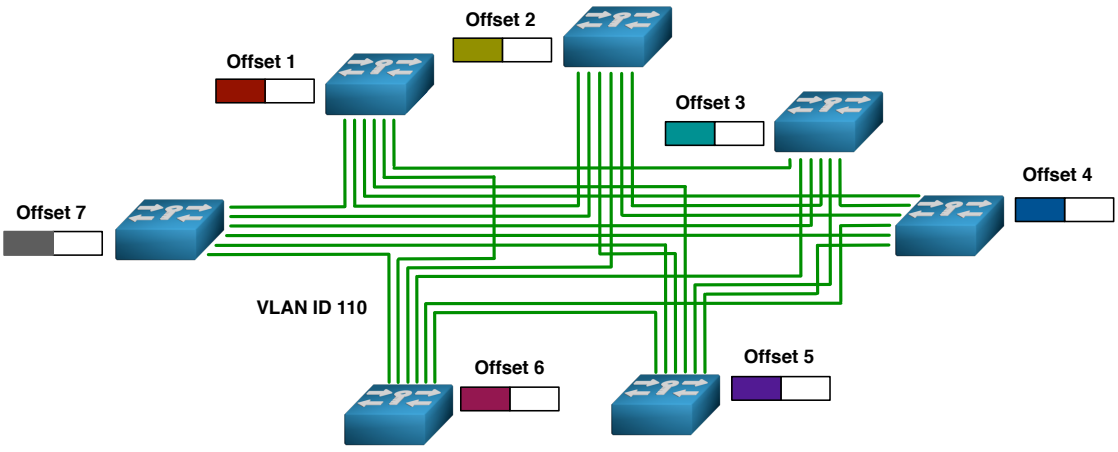


1.3. Auswirkungen des Verschlüsselungsmodus auf Funktionalitätsanforderungen

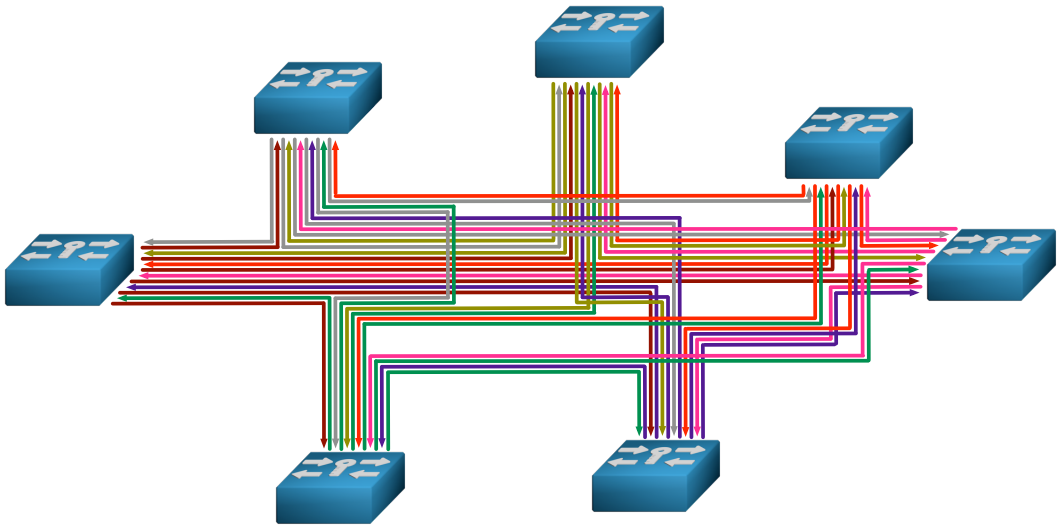
Authentisierte Verschlüsselung und der Tunnel-Modus erhöhen die Framegrösse. Bei den meisten Carrier Ethernet-Netzwerken werden Frames bis zu einer Grösse von 1600 Bytes problemlos akzeptiert. Probleme kann es nur bei den Carriern geben, welche die Empfehlungen des Metro Ethernet Forums (MEF) nicht korrekt umgesetzt haben.
Wo die Framegrösse aber eine Rolle spielen kann, ist beim Transport von Ethernet over IP im Fall wo die zulässige Maximum Transfer Unit (MTU) überschritten wird. Ein Verschlüssler sollte dies kompensieren können, indem er Frames mit Übergrösse fragmentiert. Das wiederum erfordert zusätzliche Funktionalität des Verschlüsslers.

Authentisierte Verschlüsselung erhöht auch die Anforderung bei Gruppenschlüsselsystemen. Ursache dafür ist der Counter, der unter anderem sicherstellt, dass Frames nur in der richtigen Reihenfolge oder mit minimalen Abweichungen akzeptiert werden. Da mehrere Gruppenmitglieder mit dem gleichen Schlüssel verschlüsseln ist ohne besondere Massnahmen die Kontinuität des Counters nicht gewährleistet.

Diese Problematik kann unterschiedlich gelöst werden. Ein Ansatz ist, jedem Verschlüssler einen Counter-Offset zuzuweisen und den verwendeten Counter Offset innerhalb des SecTag mitzuführen. Die empfangenden Verschlüssler wissen so um den verwendeten Offset und berücksichtigen diesen bei der Überprüfung der Einhaltung der korrekten Reihenfolge.



Ein anderer Ansatz ist, die Schlüsselzuweisung auf den versendenden Verschlüssler abzustellen und alle von diesem Verschlüssler ausgehenden Frames mit dem gleichen Schlüssel zu verschlüsseln. Für jeden Verschlüssler sind die ausgehenden Frames eine Punkt-zu-Multipunkt-Verbindung. Im SecTag wird die entsprechende Security Association mitgeführt, so dass die empfangenden Verschlüssler wissen, welchen Schlüssel sie zum entschlüsseln verwenden müssen.



1.4. Auswirkungen des Anfangsgeheimnisses auf die Mehrmandantenfähigkeit

Für das Anfangsgeheimnis kommen sowohl ein X.509 Zertifikat als auch ein Pre-Shared Secret in Frage. Zertifikate werden von einer Certificate Authority (CA) ausgestellt und auch von dieser bewirtschaftet. Liegt die Schlüsselhoheit beim Mandanten, so müsste eigentlich auch das Anfangsgeheimnis in Form eines Zertifikats von der CA des Mandanten stammen. Dafür müsste der Verschlüssler des Dienstleister nicht nur Zertifikate seiner eigenen CA, sondern auch Zertifikate anderer CAs akzeptieren. Zudem muss in diesem Fall das Zertifikat von der CA des Mandanten bewirtschaftet werden. Mit Pre-Shared Secrets ist diese Problematik nicht so ausgeprägt.

2. Abstrahlsicherheit

Elektronik verursacht Abstrahlungen. Aus diesen vorwiegend elektromagnetischen Abstrahlungen können unter Umständen mittels geeigneter Gerätschaften Daten ermittelt werden. Unter dem Namen TEMPEST gibt es von der NSA eine Spezifikation in Bezug auf Spionagemethoden basierend auf dem Aufzeichnen von elektromagnetischen Abstrahlungen, dem Aufzeichnen von Geräuschen und mechanischen Vibrationen. Diese Spezifikationen umfasst gleichzeitig auch geeignete Schutzmassnahmen vor solchen Spionageangriffen.

Bei Verschlüsslern kann der Schutz einerseits über das Gehäuse und andererseits durch Infrastrukturschutz erfolgen.

3. Übermittlungssicherheit (TRANSEC)

Das Abhören von Netzwerken kann man nicht verhindern. Authentisierte Verschlüsselung stellt die Vertraulichkeit der übermittelten Daten und des Netzwerks sicher, der Netzwerkwerkverkehr bleibt aber sichtbar. Damit sich nicht mittels Traffic Analysis herausfinden lässt, was sich auf dem Netzwerk abspielt, gibt es Traffic Flow Security. Diese vernebelt den Netzwerkverkehr. Traffic Flow Security kann unterschiedlich implementiert werden. Ältere Ansätze verwenden eine Kombination aus Frame-Verschlüsselung und fixer Framegrösse. Der Nachteil liegt darin, dass dies nur über direkte Verbindungen im Punkt-zu-Punkt-Betrieb funktioniert und in Bezug auf Overhead und Latenz nicht gerade optimal ist. Die neusten Entwicklungen erlauben die Vernebelung des Netzwerkverkehrs in drei unterschiedlichen Verschlüsselungsmodi – Frame, Transport und Tunnel – und in allen Topologien: Punkt-zu-Punkt, Punkt-zu-Multipunkt und Multipunkt-zu-Multipunkt. Mittels einer Kombination von Gruppierung von Frames und nichtssagendem Zusatzverkehr wird eine erfolgreiche Traffic Analysis verhindert, ohne dass die Netzwerkkompatibilität darunter leidet. Die Gruppierung von Frames hat zudem positive Auswirkungen auf die Netzwerkeffizienz, da gruppierte Frames nur einmal authentisiert werden müssen und auch der Interframe Gap zwischen den gruppierten Frames wegfällt. Das Gruppieren von Frames bedingt die Verwendung eines Tunnel-Modus (native, EoIP oder MPLS) und ist am effizientesten, wenn ausschliesslich Frames zwischen zwei Standorten verschlüsselt werden. Je mehr Standorte mit Verschlüssler verbunden sind, desto seltener gibt es Frames, die gruppiert werden können.

4. Infrastrukturschutz

Der Verschlüssler selbst muss bei einem Manipulationsversuch den Schlüsselspeicher inklusive der Anfangsgeheimnisse umgehend unwiderruflich löschen können. Die ganze durch den Verschlüssler gewährte Sicherheit kommt aber nur zum tragen, wenn der Verschlüssler sich an einem geschützten Ort befindet.

Die wichtigsten Fragen:

- Wie viel Sicherheit brauche ich?
- Ist der Verschlüssler manipulationsresistent?
- Wie funktioniert das Schlüsselsystem? Ist es symmetrisch, asymmetrisch oder hybrid?
- Wie kommen die Anfangsgeheimnisse auf den Verschlüssler?
- Erfolgt die Zufallszahlengenerierung in spezieller Hardware?
- Wie werden die Schlüssel erstellt, geprüft und ausgetauscht?

- Ist der Schlüsselspeicher manipulationssicher?
- Ist die Verschlüsselung authentisiert?
- Verfügt der Verschlüssler über ein Gruppenschlüsselsystem?
- Muss der Verschlüssler mandanten- oder mehrmandantenfähig sein?
- Welche Verschlüsselungsmodi brauche ich: Frame, Transport oder Tunnel?
- Brauche und habe ich die Möglichkeit, meinen Netzwerkverkehr zu vernebeln?
- Brauche ich Abstrahlsicherheit?

SINA® L2 Box

Leitungsverbindungen, so sicher, dass Angreifern das Lachen vergeht.

Sichern Sie Ihren Datenverkehr mit SINA L2 Technologie.
Die Übertragung unternehmensinterner Daten über öffentliche Leitungswege ist ein beliebter Ansatzpunkt für Angreifer und Datenspione. Schützen Sie Ihre Informationen und verschlüsseln Sie Verbindungen zwischen Standorten oder Rechenzentren mit SINA L2 Boxen – mit einem Datendurchsatz von bis zu 10 GBit/s bei weniger als 4 µs Latenzzeit. Funktionalität und Leistung Ihrer Netzinfrastruktur bleiben durch die einfache Einbindung der Boxen zwischen Firmennetz und Provider unberührt.
So haben Angreifer bei Ihnen nichts mehr zu lachen.

Klingt unmöglich? Testen Sie uns!
www.sinalayer2.secunet.com

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

Sektion 3: Betrieb

Dedizierte Verschlüssler werden oft als „Deploy & Forget“ angepriesen. Mit „Plug & Play“ darf man das allerdings nicht gleichsetzen. Vielmehr handelt es sich bei einem Verschlüssler um einen dedizierten Rechner, der aufgesetzt werden muss. Ist der Verschlüssler einmal konfiguriert und fallen keine betriebsbedingten Änderungen an, so sind tatsächlich bis auf den periodischen Austausch des Anfangsgeheimnisses in der Regel keine Wartungsarbeiten nötig. Im Wartungsfenster für den periodischen Austausch des Anfangsgeheimnisses und von Passwörtern lassen sich auch Firmware-Upgrades bewerkstelligen. Standortverbindungen sind selten Änderungen unterworfen, weshalb kaum Wartungsfenster für Konfigurationsänderungen benötigt werden.
Aus betrieblicher Sicht sind folgende Bereiche relevant: Die Konfiguration, der Einsatz, die Überwachung und die Wartung. Ein wichtiger Faktor ist dabei die Benutzerverwaltung.

1. Konfiguration

Verschlüssler sind Netzwerkgeräte und müssen in das bestehende Netzwerk integriert werden. Die Initialkonfiguration des Verschlüsslers erfolgt in der Regel lokal. Dabei gibt es unterschiedliche Vorgehensweisen, die alle den gleichen Zweck verfolgen: Die sichere Initialisierung und Konfiguration des Verschlüsslers.
Ein Ansatz besteht darin, die Konfigurationsdaten per Smartcard in den Verschlüssler einzulesen. Dafür wird für jeden der Verschlüssler zentral eine Smartcard mit seinen Konfigurationsdaten versehen. Die Smartcards werden zu den jeweiligen Verschlüsslern transportiert und dort eingesetzt. Ein anderer Ansatz ist das Verbinden eines PCs über einen seriellen oder einen Management-Port des Verschlüsslers und die lokale Konfiguration via Software. Eine weitere Möglichkeit besteht in der Kombination aus Eingaben am Frontpanel des Verschlüsslers und der Konfiguration mittels Smartcard oder Software.

Erst nach der Initialkonfiguration des Verschlüsslers können Benutzerberechtigungen erstellt und spezifischen Rollen zugewiesen werden. Vorzugsweise ist dabei das Netzwerkmanagement getrennt vom Sicherheitsmanagement. Je granularer die Rollenzuweisungen und Berechtigungen, desto besser. Schliesslich sollte sich auch die Verwaltung der Verschlüssler nahtlos an die vorhandenen Strukturen anpassen lassen.

2. Einsatz

Verschlüssler sind erst nach vollständiger Konfiguration einsatzbereit. Bis zu diesem Zeitpunkt blockieren die meisten Verschlüssler sämtlichen ausgehenden Verkehr. Bei korrekter Konfiguration arbeitet der Verschlüssler nach Inbetriebnahme transparent. Allfällige Konfigurationsänderungen erfolgen nach dem gleichen Prozedere wie die Erstkonfiguration.
Verschlüssler leiten Informationen über Verbindungsverluste (Link Loss) weiter, so dass die Plazierung des Verschlüsslers im Netzwerk keinen Unterbruch der Mitteilungskette zur Folge hat.

3. Überwachung

Mittels SNMP lässt sich der laufende Betrieb des Verschlüsslers überwachen. Systemmeldungen kann man an einen Syslog Server übermittelt werden. Lokale Event und Audit Logs zeichnen zudem relevante Vorgänge auf und lassen sich bei Bedarf abrufen.
Die Verschlüssler können sich auch gegenseitig überwachen und den Ausfall eines Verschlüsslers melden. Dafür braucht es die Funktionalität der „Dead Peer Detection".

4. High Availability

Bei betriebskritischen Netzwerkverbindungen gibt es verschiedene Möglichkeiten, sich gegen allfällige Geräte- und Netzwerkausfälle zu wappnen. Netzwerke werden in der Regel redundant ausgelegt: Fällt das eine Netzwerk auf Carrier-Seite aus, so kann auf ein zweites Netzwerk zugegriffen werden, das über einen anderen Carrier läuft. Mittels High Availability (HA) - einer Kombination aus Hard- und Software – können auch Verschlüssler redundant ausgelegt werden, so dass beim Ausfall eines Verschlüsslers automatisch ein Reservegerät übernimmt.

5. Wartung

Syslog, Event Log und im schlimmsten Fall die Status-LEDs des Frontpanels weisen auf ungeplanten Wartungsbedarf hin. Mechanische Defekte wie z.B. ein defekter Lüfter treten in der Regel genauso selten auf wie elektronische Defekte. In der Regel ist deshalb die Wartung auf die periodischen Änderungen des Anfangsgeheimnisses und von Passwörtern beschränkt.

Wichtigste Fragen:

- Wie statisch ist die Anzahl meiner Standortverbindungen?
- Wie komplex sind die Konfiguration und allfällige Konfigurationsänderungen?
- Wie aufwendig ist der Austausch von Anfangsgeheimnissen und Passwörtern?
- Wie gross sind der Schulungsaufwand und die Abhängigkeit von externen Ressourcen?
- Wie lassen sich die Verschlüssler in mein bestehendes Netzwerkmanagement integrieren?
- Wie ist die Benutzerverwaltung gestaltet: Wie viele Rollen und Hierarchien gibt es

und wie granular sind Rechte zuweisbar?
- Gibt es ein lokales Event und Audit Log?
- Wie viel Wartungsbedarf besteht?
- Muss High Availability gewährleistet sein?

Sektion 4: Netzwerk-Overhead, MTU, Latenz und Jitter

Leistungsumfang. Sicherheit und Geschwindigkeit kosten. Will man eine Lösung, die wenig kostet, so muss man zumindest bei der Sicherheit und Leistungsumfang Abstriche machen.

Aus Netzwerksicht sind Netzwerk-Overhead, MTU, Latenz und Jitter essentielle Kriterien. Sicherheit führt zwangsläufig zu Netzwerk-Overhead, da einerseits die Verschlüssler untereinander kommunizieren und andererseits die Absicherung jedes einzelnen Frames die Framegrösse erhöht. Die Vergrösserung der Frames kann dabei eher zu Problemen führen als der durch die Kommunikation zwischen den Verschlüsslern erzeugte Zusatzverkehr. Authentisierte native Verschlüsselung erhöht jeden Frame um 24 bis 40 Bytes. Dies ist abhängig von der Länge des herstellerspezifischen SecTags und vom verwendeten Verschlüsselungsmodus (Transport oder Tunnel). Im Normalfall ist diese Vergrösserung unproblematisch, da Carrier Ethernet MTUs von mindestens 1600 Bytes unterstützt. In der Regel unterstützt Carrier Ethernet auch Jumbo Frames mit Grössen von bis zu 9000 Bytes. Es gibt aber auch Carrier die weder eine MTU von mindestens 1600 Bytes noch Jumbo Frames von bis zu 9000 Bytes unterstützen. In einem solchen Fall muss die MTU kundenseitig der vom Carrier-Netzwerk unterstützten Grösse angepasst werden. Normalerweise erfolgt dies in den lokalen Standortnetzen selbst. Eine andere Lösung ist das Fragmentieren von sporadischen Übergrössen durch den sendenden Verschlüssler und das Wiederzusammensetzen durch den oder die empfangenden Verschlüssler.

Bei FPGA-basierten Verschlüssler ist die Verarbeitungszeit marginal und bewegt sich im Bereich von Mikrosekunden. Die durch die Ver- und Entschlüsselung erzeugte Latenz ist deshalb vernachlässigbar. Bei virtuellen Appliances dauert die Verarbeitung länger, was sich entsprechend negativ auf die Latenz auswirkt.
FPGA-basierte Verschlüssler bieten eine gleichmässig geringe Latenz und erzeugen deshalb keinen Jitter. Bei virtuellen Appliances kann es hingegen aufgrund der unterschiedlichen Verfügbarkeit von geteilten Ressourcen durchaus zu ungleichmässiger Latenz und damit zu unerwünschtem Jitter kommen.

Einige Verschlüssler bieten zusätzlich zu den normalen Netzwerk- und Sicherheitsfunktionen auch zweckorientierte Netzwerkfunktionalität, in den Bereichen MTU und Traffic Flow Optimization. Hervorzuheben sind primär Fragmentierung/Defragmentierung und die Kompensation des Sicherheits-Overheads durch Bündelung von kleinen Frames in Kombination mit Traffic Flow Security. Die Bündelung von Frames beding die Nutzung eines Tunnel-Modus (Ethernet Tunnel-Modus, EoIP oder MPLS).

Sektion 5: Funktionalität, Sicherheit, Geschwindigkeit und Kosten

Funktionalität. Sicherheit und Leistungsfähigkeit kosten. Will man eine Lösung, die wenig kostet, so muss man zumindest bei der Sicherheit und Funktionalität Abstriche machen. Ein hoher Preis korreliert allerdings nicht in jedem Fall mit hoher Leistungsfähigkeit, extensiver Funktionalität und hoher Sicherheit.

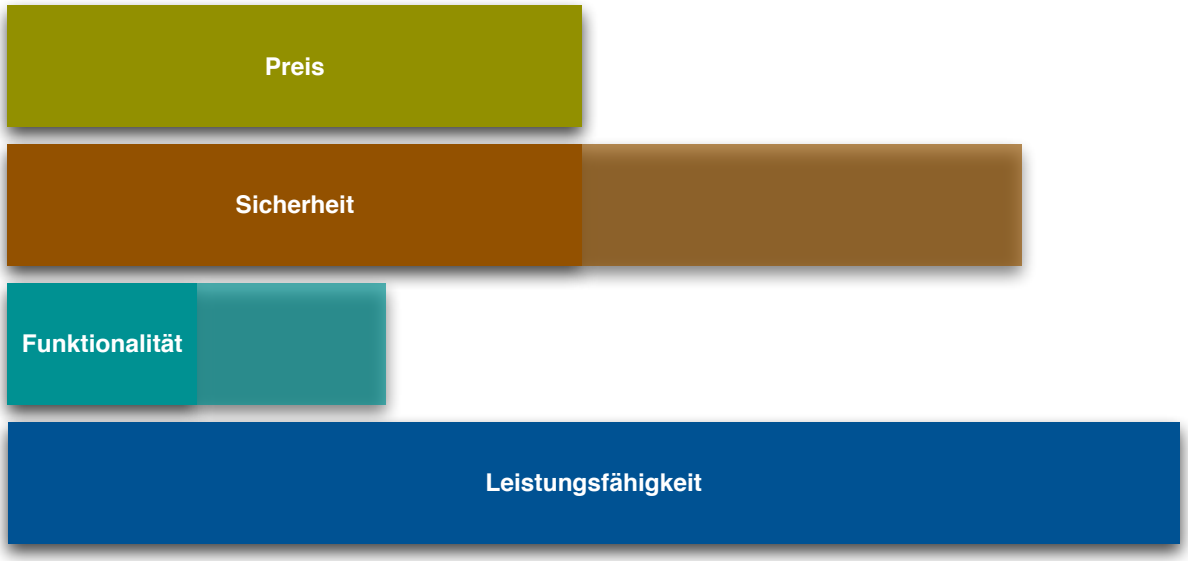
1. Unterschiedliche Ansätze

Viele Leute denken immer noch, dass MACSec der Verschlüsselungsstandard für Ethernet ist und vergessen dabei, dass MACSec für Ethernet-LANs und nicht für Ethernet-WANs entwickelt wurde. Ziel war es dabei eine kostengünstige und schnelle Lösung für LANs zu haben, welche direkt auf einer Ethernet-Karte implementiert werden kann. In Bezug auf die Verwendung von authentisierter Verschlüsselung nahm MACSec auch eine Vorreiterrolle ein. Zur Kostensenkung gespart wurde aber bei den Anforderungen in Bezug auf Schlüsselsicherheit und in Bezug auf das Schlüsselsystem. Das Resultat ist ein günstiger Preis, verbunden mit hoher Verarbeitungsgeschwindigkeit. Gespart wurde bei der Sicherheit und der Funktionalität. MACSec ist auf Hop-to-Hop ausgelegt und nicht auf End-to-End. Befinden sich zwischen den beiden verschlüsselnden integrierten Appliances weitere Netzwerkgeräte – was in der Regel der Fall ist – so sollten diese MACSec besser nicht kennen und beherrschen. Sonst könnte eines der beiden folgenden Szenarios eintreffen: Bei fehlender Connectivity und Security Association ist die Wahrscheinlichkeit gross, dass das empfangende Gerät die Annahme der Frames verweigert. Für den Fall, dass die Frames trotzdem angenommen werden besteht das Risiko, dass das Gerät den MACSec Ethertype erkennt und versucht den Frame zu entschlüsseln, obwohl keine Security Association mit dem Gerät besteht. Da dies deshalb nicht klappen kann, besteht die Gefahr, dass der Frame weggeworfen wird.
Aufgrund der Auslegung von MACSec auf LANs können sich zudem bereits im MAN-Bereich zusätzliche Probleme aufgrund von CoS und dem Verhalten von Provider Bridges in Bezug auf die Neuordnung der Reihenfolge der Frames ergeben.

MACSec als integrierte Lösung

Würde man jetzt im Vergleich eine MACSec-basierte Appliance - wie zum Beispiel einen auf den Ethernet Security Specifications (ESS) der NSA beruhenden Verschlüssler - anschauen, so wäre das Resultat anders. Zu beachten ist insbesondere, dass trotz des eingeschränkten Funktionsumfangs der ursprüngliche Preisvorteil von MACSec durch die Kosten einer Implementierung als FPGA-basierten Appliance fast vollständig wegfällt.

MACSec-basierter dedizierter Verschlüssler



Während die Sicherheit aufgrund der Verschlüsselung in einem FPGA, der sicheren Schlüsselgenerierung, der sicheren Schlüssellagerung und der Traffic Flow Security deutlich gesteigert wird, hängt vieles noch von der Sicherheit des Key Server ab. Dieser Gewinn an Sicherheit hat aber seinen Preis. ESS weicht zusätzlich noch von MACSec ab, indem es unterschiedliche Verschlüsselungsoffsets unterstützt. Die Funktionalität ist deshalb verbessert, während die Interoperabilität verringert ist. Das Schlüsselsystem bleibt aber auf Punkt-zu-Punkt und Punkt-zu-Multipunkt beschränkt und es sollte kein MACSec-fähiges Gerät zwischen den Verschlüsslern stehen.

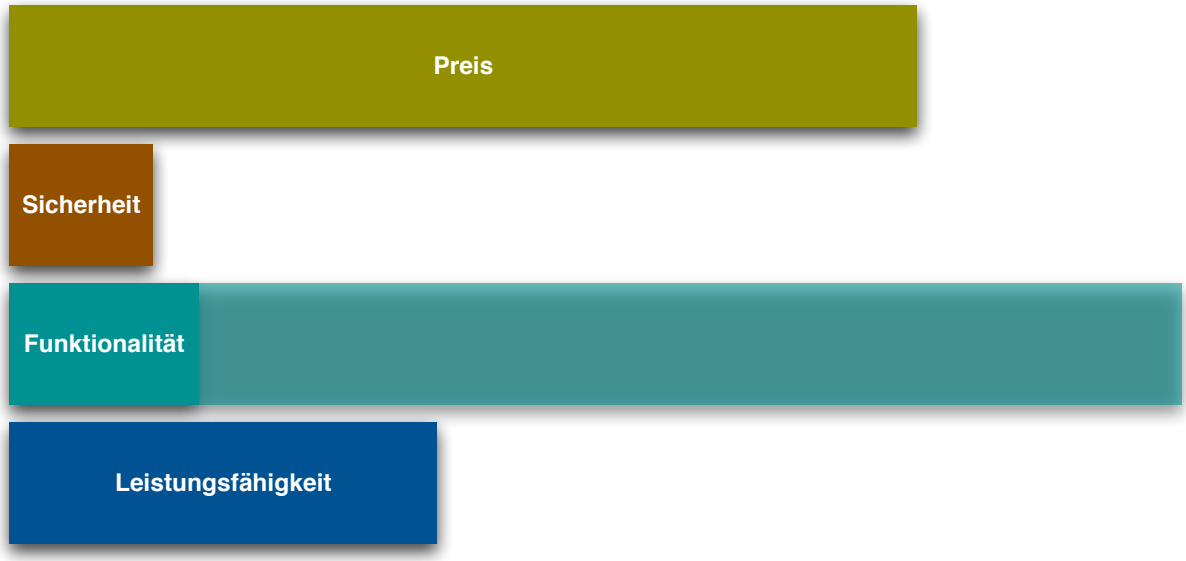
Ein weiterer Ansatz, der tiefere Kosten verspricht, ist Virtualisierung: Der Verschlüssler als virtuelle Appliance in einer virtualisierten Umgebung. Sozusagen eine Reinkarnation im Reich der Network Function Virtualization (NFV). Was auf den ersten Blick einleuchtend scheint, ist auf den zweiten Blick doch nicht mehr soll toll. Das Problem der Schlüsselsicherheit - sowohl der Generierung wie auch der Lagerung - ist ungelöst und auch in Bezug auf die Latenz mag eine virtuelle Appliance kaum zu überzeugen. Die Funktionalität kann aber durchaus hoch sein.

Theoretisch kann jeder Verschlüssler, der auf einer x86-CPU basiert, auch auf einer virtuellen x86-CPU laufen. Der Verschlüssler läuft dann als Applikation auf einer virtuellen Maschine (VM). Zwischen einer echten und einer virtuellen Appliance gibt es aber einige wichtige Unterschiede, die berücksichtigt werden müssen. So fehlen neben dem physischen Geräteschutz auch die benötigte Entropiequelle für die hardware-basierte echte Zufallszahlenerzeugung und der manipulationssichere Schlüsselspeicher. Der physische Geräteschutz muss durch einen äquivalenten physischen Schutz des Servers kompensiert werden, während die für Schlüsselerzeugung und -lagerung notwendige Hardware entweder über eine lokale Smart Card oder über ein netzwerk-basiertes Hardware Security Module (HSM) zur Verfügung gestellt wird. Die lokale Smartcard wird am Host über USB angeschlossen und kann von der virtuellen Appliance, die auf dem Host läuft, angesprochen werden. Die benötigte Sicherheit und der geforderte Schutz sind so auch bei einer virtuellen Appliance vorhanden, aber eben nur, falls die entsprechende Hardware nicht nur virtuell, sondern auch reell vorhanden ist.

Die Performance der virtuellen Appliance ist von mehreren Faktoren abhängig. Dazu gehören die Hardware-Ausstattung des physischen Hosts, die Leistungsfähigkeit des Hypervisors, die Anzahl der nebst der virtuellen Appliance auf dem Host laufenden virtuellen Maschinen (VMs) und die CPU-, Speicher- und I/O-Belastung durch die anderen virtuellen Maschinen. Die Virtualisierung bringt es mit sich, dass die bestehenden Hardware-Ressourcen geteilt werden und zu einem Zeitpunkt jeweils nur einer virtuellen Maschine zur Verfügung stehen. Werden mehrere Echtzeitdienste auf dem gleichen Host in unterschiedlichen virtuellen Maschinen betrieben, so hat das zwangsläufig Auswirkungen auf Latenz und Jitter.
Die Sicherheit der virtuellen Appliance hängt von mehreren externen Faktoren ab: Einerseits muss der Server, auf dem die virtuelle Appliance läuft, vor unerlaubtem Zugriff geschützt sein. Andererseits bilden auch das Gastbetriebssystem, der Hypervisor und die anderen auf dem Host laufenden virtuellen Maschinen ein Sicherheitsrisiko.
Der Einsatz von virtualisierten Verschlüsslern ist deshalb auf spezifische Szenarien beschränkt. Ein typisches Beispiel wäre eine virtuelle Appliance auf einem Host, auf dem

noch Firewalls laufen. Zudem macht es nur dort Sinn, wo der zu verschlüsselnde Datenverkehr im unteren Bereich, d.h. zur Zeit unter 50-70 Mbit/sec liegt und die im Vergleich zu einer dedizierten Appliance erhöhte Latenz und der grössere Jitter keine unerwünschten Nebenwirkungen zur Folge haben. Performancemässig sinkt die Leistungsfähigkeit gemessen an Latenz und Jitter bei grösseren Bandbreiten auf die Werte, die man sich bei softwaremässig implementierten IPSec-Verschlüsslern gewohnt ist. Problematisch sind in erster Linie Echtzeit-Dienste (e.g. IP-Telephonie).

Virtuelle Appliance



Bei einer dedizierten und spezialisierten Appliance sieht das Profil anders aus. Der Preis liegt etwas höher als bei einer dedizierten Appliance, die auf MACSec aufbaut. Die Leistungsfähigkeit ist top, sowohl in Bezug auf Bandbreite wie auch in Bezug auf Latenz. Sichere Schlüssel und ein multipunktfähiges Schlüsselsystem bieten alle Hersteller. Differenzen in der Sicherheit bestehen vorwiegend in Bezug auf die gebotenen Verschlüsselungsmodi und Traffic Flow Security. Bei der Funktionalität gibt es grössere Unterschiede in Bezug auf Mandanten- und Mehrmandantenfähigkeit und Netzwerkunterstützung.

Dedizierte Appliance

2. Abwägungen

Billig und sicher schliessen sich gegenseitig aus. Funktionalität kostet auch Geld. Geht es rein um den Preis und die Geschwindigkeit bei geringem Sicherheitsbedarf und minimalen Funktionalitätsanforderungen, so sind MACSec-basierte integrierte Appliances ein kostengünstiger Weg. Zumindest solange die Basisdienste von MACSec genügen. Aufgrund der beschränkten Funktionalität kann MACSec zu höheren Netzwerkosten führen, die sich nicht als CapEx, sondern als OpEx bemerken machen.
Hohe Sicherheit und umfassende Funktionalität bei hoher Verarbeitungsgeschwindigkeit bieten nur spezialisierte Verschlüssler. Bei mandanten- und mehrmandantenfähigen Systemen besteht auch die Möglichkeit, die Verschlüsselung als Dienstleistung zu beziehen, ohne dabei die Schlüsselhoheit aus der Hand zu geben. So fallen die Anschaffungskosten weg und es fallen nur Betriebskosten an.

3. Evaluation

Um die verschiedenen Alternativen und Angebote bewerten zu können, ist es von Vorteil, wenn man die eigenen Anforderungen in Bezug auf Netzwerk und Sicherheit kennt. Die nachfolgenden Checklisten helfen bei der Definition der Anforderungen und erlauben eine zielgerichtete Evaluation der verfügbaren Lösungen.


thales-esecurity.com
Datacryptor®
High performance security for data in motion
Everywhere it matters, we deliver
MAN IN THE MIDDLE THREAT PROTECTION
Leverage Galois Counter Mode (GCM) to guard encrypted data against packet replay
SINGLE PURPOSE SECURITY
Unlike switches and firewalls, Datacryptor is purpose-built for securing data in motion
KEY LIFECYCLE MANAGEMENT
Enable complete management control including certified hardware-based random number generation and secure key storage
HIGH PERFORMANCE
Deliver consistent, optimum security from VoIP to jumbo frames, 10Mbps to 10Gbps
REGULATORY COMPLIANCE
Protect data to reduce risk of breach
Millions of critical decisions are made every day in data protection. Thales is at the heart of this, with more than 40 years' experience. Our customers rely on integrated smart technologies such as Datacryptor® to protect the confidentiality, integrity and availability of sensitive information. Our products, services and solutions help businesses and governments reduce risk, demonstrate compliance, enhance agility and make more effective responses in critical environments. Everywhere, together with our customers, we are making a difference.
THALES
Together • Safer • Everywhere

Anhang:

Checkliste zur Evaluation von Verschlüsslern für Metro und Carrier Ethernet

Version 1.0

Sektion 1: Netzwerk und Einsatzszenario

1. Unterstützte Netzwerktopologien

Wie sieht die Topologie des zu schützendes Netzwerks aus?

Punkt-zu-Punkt (2 Standorte) ☐
Punkt-zu-Multipunkt (mehrere Standorte) ☐
Multipunkt-zu-Multipunkt (mehrere Standorte) ☐

Geschichtete Netzwerktopologien ☐

Sind Topologieänderungen in den nächsten fünf Jahren wahrscheinlich? ☐

2. Anzahl Standorte

Wie viele Standorte sollen miteinander verbunden werden?

2 ☐
2-10 ☐
11-25 ☐
26-50 ☐
50+ ☐

3. Netzwerk – Nur Ethernet oder gemischt?

Ist das Netzwerk in sich geschlossen oder werden an den Standorten auch Zugänge für IP und MPLS benötigt?

In sich geschlossenes Carrier –Ethernet-Netzwerk ☐
Ein- und Ausgang für andere Netzwerke (MPLS, IP) ☐

4. MTU

Wie gross ist die unterstützte MTU für Carrier Ethernet seitens Carrier? ..... bytes
Wie gross ist die unterstützte MTU für IP seitens Carrier ..... bytes

5. Unterstützte Einsatzszenarien

Erfolgt die Verschlüsselung inklusive Unterhalt der Verschlüssler im Eigenbetrieb oder sind Teile des Betriebs ausgelagert?

Eigenbetrieb ☐
Managed Encryption Service (mandantenfähig) ☐
Managed Encryption Service (mehrmandantenfähig) ☐
Managed Security Service (mandatenfähig) ☐
Managed Security Service (mehrmandantenfähig) ☐

5. Unterstützte Netzwerke

Ethernet ☐
MPLS über Ethernet (MPLSoE) ☐
Ethernet über IP (EoIP) ☐
MPLS über Ethernet über IP (MPLSoEoIP) ☐
IPv4 für EoIP ☐
IPv6 für EoIP ☐

6. Maximal unterstützte Bandbreite

100 Gb/sec voll-duplex ☐
40 Gb/sec voll-duplex ☐
10 Gb/sec voll-duplex ☐
1 - 2 Gb/sec voll-duplex ☐
100Mb/sec – 1 Gb/sec voll-duplex ☐
10 - 100 Mb/sec vollduplex ☐

Erhöhung der Bandbreitenunterstützung via Software-Lizenz ☐

Sektion 2: Communication Security

1. Sicherheitsanforderungen

Je nach Sicherheitsanforderungen können sich die Funktionalitätsanforderungen unterscheiden.

1.1. Tief

Ohne hardwaremässig generierte und abgesicherte Schlüssel ☐
Ohne authentisierte Verschlüsselung ☐
Integrierte Appliance ☐

1.2. Mittel

Dedizierte Appliance ☐
Mit hardware-basierter Schlüsselgenerierung und Aufbewahrung ☐
Mit authentisierter Verschlüsselung ☐
Mit zusätzlicher Authentisierung pro Gruppe ☐

1.3. Hoch

Dedizierte Appliance ☐
Mit hardware-basierter Schlüsselgenerierung und Aufbewahrung ☐
Mit authentisierter Verschlüsselung ☐
Mit zusätzlicher Authentisierung pro Gruppe ☐
Mit Unterstützung von Frame-Modus und Tunnel-Modus ☐
Traffic Flow Security (TFS) ☐
Emissionsschutz ☐

2. Crypto-Sicherheit

2.1. Schlüsselgenerierung

Echter hardwaremässiger Zufallszahlengenerator ☐
Softwaremässiger Pseudozufallszahlengenerator ☐

2.2. Schlüsselaufbewahrung

Manipulationssicherer Speicher ☐
Ungeschützter Speicher ☐

2.3. Schlüsselaustausch

Es gibt unterschiedliche Wege, Schlüssel auszutauschen. Jeder Anbieter kann den Lebenslauf eines Schlüssels im Detail aufzeigen. Ohne spezifische Nachfrage wird er dies allerdings nicht tun.

Asymmetrische Schlüssel mit symmetrischer Überschlüsselung der Teilschlüssel ☐
Asymmetrische Schlüssel ohne symmetrische Überschlüsselung der Teilschlüssel ☐
Authentisierter Schlüsselaustausch ☐
Wahl aus verschiedenen Kurven bei Verwendung von Elliptic Curve Cryptography ☐
Schlüsselaustausch in-band ☐
Schlüsselaustausch out-of-band ☐

2.4. Verschlüsselungsalgorithmus und Betriebsmodus

AES-GCM (authentisierte Verschlüsselung) ☐
AES (unauthentisierte Verschlüsselung) ☐
Anderer authentisierter Verschlüsselungsmodus ☐

2.5. Schlüsselgrösse

128 Bit (für tiefe Sicherheitsbedürfnisse) ☐
256 Bit (für mittlere und hohe Sicherheitsbedürfnisse) ☐

2.6. Verschlüsselungsmodi

Je nach Sicherheitsbedürfnis und Netzwerkunterstützung kommen unterschiedliche Verschlüsselungsmodi zum tragen.

Frame-Modus (für direkte Verbindungen und für EoIP) ☐
Transport-Modus ☐
Tunnel-Modus (zum Verstecken der Meta-Daten) ☐

2.7. Inhalt des SecTag

Im SecTag führt der Frame zusätzliche Informationen, wie zum Beispiel einen Counter, eine Security Association oder einen Counter-Offset mit sich. Je kürzer der Counter, desto öfter müssen Schlüssel gewechselt werden.

Eigener EtherType ☐
Grösse des Counters ☐

2.8. Schlüsselverwaltung und Frame-Inhalt

Der Schlüsselverwaltung stehen die im Frame mitgeführten Adressdaten, der Ethertype des unverschlüsselten Frames und die zusätzlichen Daten im SecTag zur Verfügung. Jede Schlüsselverwaltung funktioniert anders. Die Hersteller erklären gerne, wie was zusammenhängt und abläuft.

2.9. Betriebsarten des Schlüsselsystems

Je nach Einsatzszenario sind paarweise Schlüsselsysteme oder Gruppenschlüsselsysteme vorzuziehen. Ein Verschlüssler sollte beide Möglichkeiten bieten. Bei Gruppenschlüsselsystemen sollte darauf geachtet werden, wie die Gruppen definiert sind respektive definiert werden können.

Paarweises Schlüsselsystem ☐
Gruppenschlüsselsystem ☐

2.10. Schlüsselzuweisung

Je nach Netzwerk und Topologie wird eine port-basierte oder eine VLAN-basierte Schlüsselzuweisung benötigt.

Port-basiert ☐
VLAN-basiert ☐
Gruppen-basiert ☐

2.11. Skalierbarkeit

Die Skalierbarkeit ist nicht nur abhängig von der Anzahl Standorte, sondern auch von der Anzahl VLANs. Da jedes VLAN eine Gruppe darstellt und einzeln authentisiert werden sollte, ist bei zertifikatsbasierter Authentisierung die Anzahl Zertifikate, die ein Verschlüssler maximal verwenden kann, oft eine einschneidendere Limitation als die Anzahl Standorte.

< 50 Gruppen/VLANs ☐
> 50 Gruppen/VLANs ☐

2.12. Key Server

Key Server können entweder in jeden Verschlüssler eingebettet oder eigenständige Geräte sein. Nachteil von Einzelgeräten ist die Verringerung der Ausfallsicherheit, die mit geeigneten Massnahmen kompensiert werden muss. Bei grösseren Netzwerken kommen oft hybride Konfigurationen zum Einsatz.

Eingebetteter Key Server ☐
Dedizierter Key Server ☐
Hybrid eingebettet/dediziert ☐

3. Transmission Security, Ausstrahlsicherheit und Infrastrukturschutz

Ohne Transmission Security, kann mittels Traffic Flow-Analyse der Netzwerkverkehr unter die Lupe genommen werden. Traffic Flow Security ist deshalb bei kritischen Standortverbindungen mit hohen Sicherheitsanforderungen eine äusserst nützliche Funktionalität. Ausstrahlsicherheit spielt primär da eine Rolle, wo der Infrastrukturschutz nicht in der Lage ist, den Bereich mit den Verschlüsslern so abzusichern, dass keine Unbefugten Zutritt haben und dass keine elektromagnetischen Strahlen austreten.

Traffic Flow Security ☐
Ausstrahlsicherheit ☐

Sektion 3: Netzwerk

Bei einem Netzwerkverschlüssler spielen die Netzwerkeigenschaften eine genauso wichtige Rolle wie die Sicherheit.

1.1. Verschlüsselungsoffset

Ethernet-Frames können unterschiedliche Daten mit sich führen. Je nach Netzwerk und da insbesondere bei MPLS-Netzwerken, darf der Verschlüsser nicht bereits nach der ersten VLAN-ID mit der Verschlüsselung beginnen. Die Verschlüsselung beginnt in einem solchen Fall erst nach einem Offset.

Fix setzbarer Verschlüsselungsoffset ☐
Fix setzbarer Verschlüsselungsoffset per VLAN oder Gruppe ☐
Automatisches Bestimmen des Verschlüsselungsoffset nach Inhalt ☐

1.2. Konditionelle Verschlüsselung

Je nach Einsatzszenario und Position des Verschlüsslers im Netzwerk dürfen nicht alle Frames verschlüsselt werden. Das kann sich z.B. auf VLAN-IDs, Frames mit einem spezifischen Ethertype oder Frames mit MPLS-Tag beziehen.

Ausschluss basierend auf MAC-Adresse ☐
Ausschluss basierend auf VLAN-ID ☐
Ausschluss basierend auf EtherType ☐
Ausschluss basierend auf Gruppenzugehörigkeit ☐
Ausschluss basierend auf Präsenz von MPLS-Tag ☐
Ausschluss basierend auf Kombination mehrerer Kriterien ☐

1.3. Latenz und Jitter

Latenz und Jitter hängen direkt von der verwendeten Verschlüsselungshardware ab. FPGA und ASIC verarbeiten Daten schneller als eine CPU, aber nur FPGA und CPU erlauben eine Aktualisierung der Software ohne Hardwaretausch. Virtuelle Appliances tendieren bei höheren Geschwindigkeiten zu Jitter.

FPGA & CPU ☐
ASIC ☐
CPU ☐

1.4. MTU

Das Verhalten des Verschlüsslers in Bezug auf die MTU spielt in mehrfacher Hinsicht eine Rolle. Auf der einen Seite ist das die maximal unterstützte Framegrösse und auf der anderen Seite ist es das Verhalten bei übergrossen Frames.

Unterstützung von Jumbo Frames ☐
Fragmentierung/Defragmentierung überlanger Frames ☐

1.5. Ethernet Flow Control

Ethernet Flow Control gehört bei einem guten Switch zut Standardfunktionalität, insbesondere die Unterstützung von „Pause“. Damit lässt sich übermässiges Datenaufkommen von einer Gegenstelle kurzfristig reduzieren, um einen guten Verkehrsfluss zu garantieren.

Unterstützung Ethernet Flow Control (Pause) ☐

1.6. Out-of-Order Handling

Theoretisch kommen in einem Netzwerk Frames in der Reihenfolge an, in der sie abgeschickt wurden. In der Praxis kommt es durchaus vor, dass die Reihenfolge durch zwischengeschaltete Geräte verändert wird. Speziell bei authentisierter Verschlüsselung mit Counter kann das zu Problemen führen. Deshalb muss ein Verschlüssler, der authentisierte Verschlüsselung beherrscht über eine Funktion verfügen, welche eine gewisse Toleranz in der Reihenfolge gewährt. Diese Toleranz wird meistens in Anzahl Frames angeben. Ein anderer Ansatz ist die Definition der Toleranz durch einen Zeitraum, beispielsweise eine gewisse Anzahl von Sekunden.

Definierbarkeit des Toleranzrahmens für Frames ausserhalb der Reihenfolge ☐

Sektion 4: Betrieb

1. Konfiguration

Je nach Hersteller funktionieren Konfiguration und Konfigurationsänderungen anders. Ohne spezifisches Nachfragen gibt es da keine Infos. Ein Aspekt, der zu wenig beachtet wird ist dabei der Aufwand für das regelmässige Auswechseln der Anfangsgeheimnisse und der Passwörter.

2. Nutzermanagement

Die Granularität der Nutzerverwaltung ist ein entscheidender Faktor bei der Sicherheit.

Rollen-basierter Zugriff ☐
Identitäts-basierte Authentifizierung des Benutzers ☐
Anzahl Hierarchieebenen ☐
Anzahl Rollen ☐
Strikte interne Trennung von Benutzern ☐
Separate Rolle für Security Officer ☐

3. Gerätemanagement

Beim Gerätemanagement ist zwischen Konfiguration und Überwachung zu unterscheiden. Wichtig ist in allen Fällen, dass der Verschlüssler sichere Versionen der Protokolle verwendet. So z.B. SNMPv3 statt dem veralteten und unsicheren SNMPv1.

3.1. Out-of-Band-Management

Das Out-of-Band-Management bedingt einen zusätzlichen Management-Port beim Verschlüssler.

Separater Management-Port ☐

3.2. In-Band-Management

Erfolgt die Verwaltung über das Netzwerk, so kommen unterschiedliche Netzwerk- und Sicherheitstechnologien zum Einsatz. Entscheidend ist nicht nur die Version einer Technologie, sondern auch die Implementierung.

SSH ☐
SNMPv3 ☐
TLS ☐
Proprietäre Protokolle ☐

4. Überwachung und Verhalten bei Verbindungs- oder Geräteausfall

Mittels SNMP kann der Betrieb der Verschlüssler überwacht werden. Fällt eine Verbindung (Link) oder ein beteiligter Verschlüssler aus, so muss ein Verschlüssler diese Informationen weiterleiten.

4.1. Überwachung

Mittels SNMP und einer geeigneten Netzwerksoftware, die in der Regel im Lieferumfang beinhaltet ist, kann der laufende Betrieb überwacht werden.

Remote Monitoring ☐

4.2. Link Loss Forward

Beim Ausfall einer Verbindung kommt es für die Weiterleitung der diesbezüglichen Informationen darauf an, ob es sich um eine Glasfaserverbindung oder eine Drahtverbindung handelt.

Optical Loss Pass-Through (nur für optische Verbindungen) ☐
Link Loss Carry Forward (für alle Verbindungen) ☐

4.3. Dead Peer Detection

Bei Ausfall einer Gegenstelle sollte ein Verschlüssler dies merken und melden.

Dead Peer Detection ☐

5. Logs

Verschlüssler unterstützen eine Mehrzahl an Logs für unterschiedliche Zwecke: Syslog für die zentralisierte Aufbereitung, ein Event Log für die lokale Analyse und ein Audit Log für die Revisoren.

Syslog-Unterstützung ☐
Event Log (lokal) ☐
Audit Log (lokal) ☐

Sektion 5: Zertifizierungen und Kosten

1. Zertifizierungen

Die meisten Zertifizierungen gewähren so viel Sicherheit und Netzwerkfunktionalität wie das Papier, auf dem sie gedruckt sind. Zu dieser Gruppe gehören FIPS und grossteils auch Common Criteria. Führend in Bezug auf die Aussagekraft einer Zertifizierung ist zur Zeit das BSI. Im Zweifelsfall ist eine BSI-Zertifizierung einer Common Criteria-Zertifizierung und insbesondere einer FIPS-Zertifizierung vorzuziehen.

2. Kosten

Bei einer kalkulatorischen Einsatzzeit von fünf Jahren sollten auch die Gesamtkosten über diesen Zeitraum berechnet und dann die monatlichen Kosten ermittelt werden. Je nach Anbieter unterschieden sich Garantiezeiten und die Kosten für Supportverträge. Das Berechnen der monatlichen Kosten für die Sicherheit zeigt das Kostenverhältnis zwischen Netzwerk und Sicherheit. Beim Bezug der Verschlüsselung als Service fallen die Kosten in der Regel monatlich oder vierteljährlich an.