InfoGuard
SWISS CYBER SECURITY

SONET/SDH ENCRYPTION

High-performance data encryption for SONET/SDH Networks

- Point-to-point Layer 1 SONET/SDH data encryption using AES
- 100% encryption performance and minimal latency < 1 µs
- Easy network integration into existing SONET/SDH networks
- Supports STM-1, STM-4, STM-16 and STM-64
- Central configuration, administration and monitoring
- Developed and manufactured in Switzerland

Modern high-speed backbone links are generally based on synchronous SONET/SDH networks. The area of applications of SONET/SDH links with transfer rates of between 155 Mbps and 10 Gbps is constantly expanding. What is often overlooked in this process, however, is the fact that such networks can be tapped and manipulated easily. If the confidentiality, integrity and authenticity of information are not fully guaranteed, users of this otherwise revolutionary technology are exposed to a threat of possibly existential proportions.

The only reasonable and reliable measure for protecting information and for meeting existing compliance requirements is to encrypt such information at the point of entry to the public network. InfoGuard provides a protocol-transparent encryption portfolio for all-round secure information exchange over optical SONET/SDH links.

SONET/SDH ENCRYPTION

High-performance encryption made in Switzerland

In day-to-day business, data transfer over fiber optic networks has become ‘de rigueur’. In more and more networks, bandwidths of up to 10 Gbps are the order of the day when linking various sites e.g. server farms and computer centers as well as for backup and disaster recovery infrastructures. Unfortunately, the prevailing opinion according to which fiber optic lines, compared with regular copper cables, are especially secure, does not hold true in practice. On the contrary: Just bending the fiber is all it takes to listen secretly to information exchange. The only reasonable and secure measure for protecting yourself against attacks of any kind is the encryption of that information without, however, jeopardizing performance in any way. InfoGuard products have been developed – in accordance with international security standards – exactly for this demanding task using an approach that is truly exemplary and innovative.

Revolutionary

Secure

Reliable

Maximum Performance
InfoGuard encryption devices are fully transparent within the network. Their outstanding performance, i.e. 100% encryption throughput, and their minimal latency of < 1 µs make it possible to use the devices even in time-critical applications and in heavy-load links.

Great Flexibility
Their flexible and modular architecture allows them to be used perfectly tap-proof in various protocols (Ethernet, SONET/SDH, Fibre Channel) in conjunction with different MAN, WAN and SAN applications at data rates of 10 Gbps.

Powerful Data Encryption
All security solutions have been developed strictly in accordance with the FIPS 140-2 level 3 requirements. Data encryption is done using the public Advanced Encryption Standard (AES) with a key length of 128 or 256 bits.

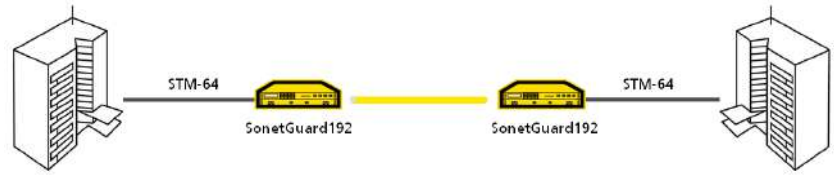
Easy Handling
Simplicity and ease of use to the benefit of security are guaranteed. The devices can be managed locally via the internal user interface or via a graphic PC user interface or remotely via a secure SSH port.

High Availability
InfoGuard products have been explicitly designed for longevity and require almost no maintenance. In order to guarantee uninterrupted service at all times, the devices are equipped with a redundant power supply. In order that users can depend on the high availability of the devices, InfoGuard provides individually tailorable maintenance services.

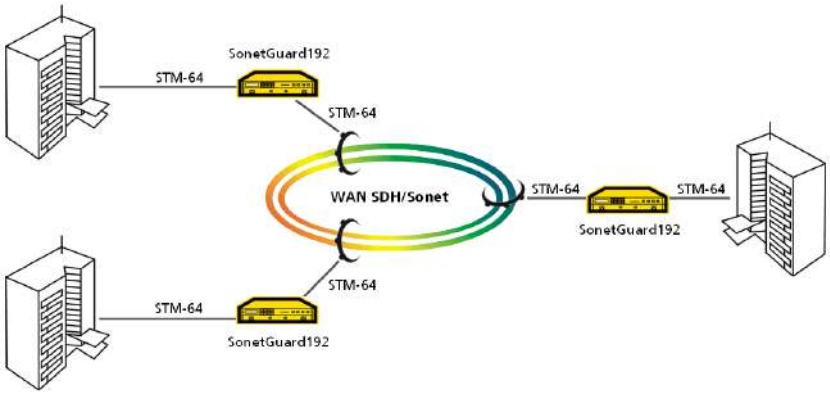
Swiss Product
As Swiss company, we can guarantee the highest quality of our products and absolute independence when implementing our security features. All security-relevant modules are developed and manufactured by our certified security specialists in Switzerland.

Dark Fiber/DWDM/CWDM

Today, large-scale Wide Area Networks (WAN) as well as Metropolitan Area Networks (MAN) are frequently SONET/SDH-based, generally employing, in addition to dedicated point-to-point links, additional CWDM and/or DWDM technologies for optimal load balancing within the existing fiber optic networks. The encryption device can be seamlessly integrated into such network topologies for comprehensive data protection throughout the transfer chain. Selecting the appropriate transceiver, users can address both passive and active CWDM/DWDM components. In addition, choosing the appropriate encryption modi is the precondition for mapping the encrypted signal onto the next higher multiplex level.



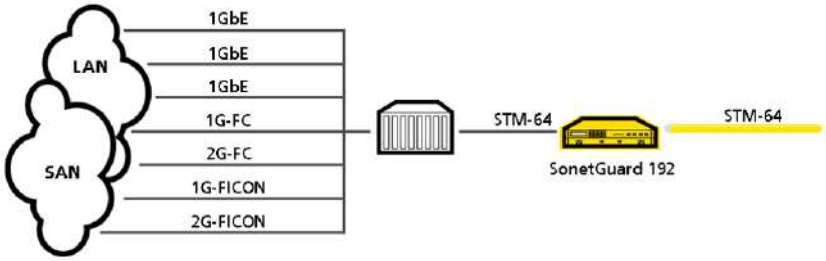
Dark Fiber



CWDM/DWDM

Time Division Multiplexing

In combination with a Time Division Multiplexing card (TDM), several low-bandwidth protocols can be transformed into a STM- signal and subsequently encrypted. Where two or more links between two sites need to be encrypted, combining a TDM card with the encryption device is a highly cost-efficient solution. On the client side, several Fibre Channel Services, FICON Services or Gigabit Ethernet Services can be fed into the system, providing users with maximum flexibility.



Time Division Multiplexing

INFOGUARD
SONET/SDH ENCRYPTION

SECURITY	
Algorithm	AES
Key length	256 Bit (Optional 128 Bit)
Key change	Automatic communication key change without interruption of traffic
Encryption mode	• Path: VC-4 Container • Line: Encryption of the entire SDH • Encryption of the Section Overhead selectable
Access protection	• Tamper proof design • Password protection, identity-based operator authentication • Block/unblock function • Emergency clear

MANAGEMENT	
Key entry	• Automatic key generation with true random generator • Copy/backup of key and installation data via SecurityCard • Manual key input via user interface
Management	• Secure remote management (SSH v2 CLI) • Inter unit management via SecurityCard – SDC-1100 • Local management via keypad and display or via via web-based user interface • Standard network management (SNMPv1/Standard MIB-II) • Audit and Event Logging

HARDWARE	InfoGuard SG192	InfoGuard SG48	InfoGuard SG12	InfoGuard SG3
Line rate	STM-64/OC-192 9.953 Gbps	STM-16/OC-48 2.488 Gbps	STM-4/OC-12 622.08 Mbps	STM-1/OC-3 155.52 Mbps
	Full Duplex, Encryption without overhead			
Communication Interface	**SFP/XFP**-Module with LC connector			
Latency	< 1 µs			
Management Interface	• Ethernet 10BASE-T/100BASE-TX RJ45 (Management) • Serial RS-232 RJ45 (Diagnostics) • RJ45 Alarm Relay (Active or Non-Active Alarm Indication)			
Test facilities	• Build-in test equipment (BITE) • Diagnostics (BITE)			
Quality system	ISO 9001:2000			
Conformity	CE (European Conformity)			
Compliance	Fulfills FIPS 140-2 level 3 requirements			
EMC	EN 55022 Cl B und EN 55024 nach 89/336/EEC-Richtlinie			
Safety	EN 60950-1 and EN 60825-1 (Class 1) according to 73/23/EEC guidelines			
Power supply	• Dual power supply unit, hot pluggable (AC/AC) • Redundant hot-swap power supply, 100V–240V AC 50...60 Hz, 48V DC • Maximum power consumption 100 W			
Operation temp.	0° C ... +50° C			
Storage temp.	-25° C ... +70° C			
Humidity	5% ... 95%			
Cooling	6 ventilators, redundancy, hot-pluggable			
Dimensions	19“ Rack-Mounting – 2 Units High, 444 x 88 x 350 mm (W/H/D)			
Weight	8.6 kg			
Reliability	MTBF 100‘000 hours			
Availability	99,999%			

InfoGuard – The Swiss Cyber Security Expert

We have many years of experience in conceiving and developing security solutions for demanding applications. All security-relevant features are developed, manufactured and implemented by our certified security specialists in Switzerland.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Switzerland
Phone +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Switzerland
Phone +41 31 556 19 00

INFOGUARD.CH