InfoGuard
and information becomes secure

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 < 1µs**
- **Easy network integration into existing STM-64 SONET/SDH networks**
- **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 solution 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.

Maximum Performance

InfoGuard encryption devices are fully transparent within the network. Their outstanding performance, i.e. 100% encryption throughput, and their minimal latency of <5µs 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 GbE.

Powerful Data Encryption

All security solutions have been developed strictly in accordance with the Common Criteria and 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

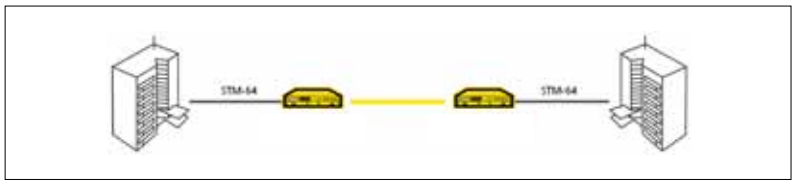
Simplicity and ease of use to the benefit of security are guaranteed. The devices can be managed locally via the internal user interface or via a graphic PC user interface or remotely via a secure SSH port.

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.

A Swiss Product

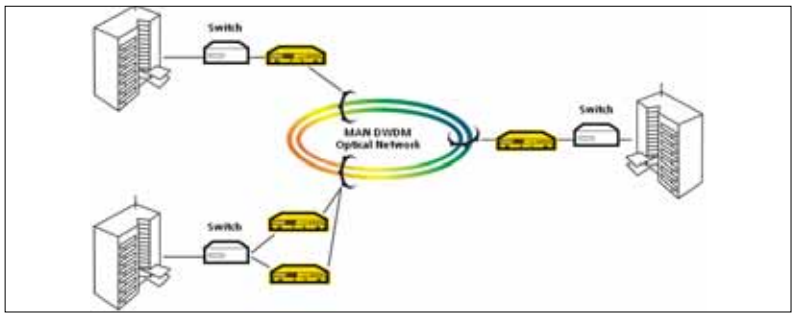
A Swiss company, we can guarantee the highest quality of our products and absolute independence when implementing our security features. All security-relevant modules are developed and manufactured by our certified security specialists in Switzerland.



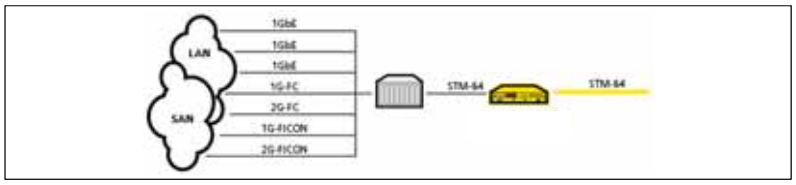
Dark Fiber

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.



CWDM/DWDM



Time Division Multiplexing

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.

Time Division Multiplexing

In combination with a Time Division Multiplexing card (TDM), low-bandwidth protocols can be transformed into a OC-192/STM-64 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 solu-tion. On the client side, several Fibre Channel Services (1, 2 or 4 Gbps), FICON Services (1 and 2 Gbps) or Gigabit Ethernet Services up to a total bandwidth of 10 Gbps can be fed into the system, providing users with maximum flexibility.

InfoGuard SG 192 –
OC-192 / STM-64 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-4-64c Container Line: STM-64/OC-192 Frame without Section Overhead
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 SG 192 – OC-192/STM-64 Encryption
Line rate	9.953 Gbps, Full Duplex, Encryption without overhead
Communication Interface	OC-192/STM-64 XFP-Module w. LC connector
Management Interface	Ethernet 10BASE-T/100BASE-TX RJ45 (Management) Serial RS-232 RJ45 (Diagnostics) RJ45 Alarm Relay (Active or Non-Active Alarm Indication)
Latency	< 1 µs
Test facilities	Build-in test equipment (BITE) Diagnostics (BITE)
Quality system	ISO 9001:2000
Conformity	CE (European Conformity)
Compliance	Designed according Common Criteria Security Standard Fulfills FIPS 140-2 level 3 requirements
EMC	EN 55022 Cl B and EN 55024 according to 89/336/EEC guidelines
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) AC input 230 VAC nominal 100 V – 240 V/50 ... 60 Hz (+/-10%) 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 (B/H/T)
Weight	8.6 kg
Reliability	MTBF 50’000 hours
Availability	99,999%

InfoGuard – Your Partner for Persuasive Security Solutions with the Swiss Seal of Quality!
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	www.infoguard.ch · info@infoguard.ch
Headquarters	Feldstrasse 1 · CH-6300 Zug/Switzerland · Phone +41 41 749 19 00 · Fax +41 41 749 19 10
Western Europe	InfoGuard Representative Office London · Phone +44 1494 772 294 · sales.west@infoguard.com
Central and Eastern Europe	InfoGuard Representative Office Frankfurt · Phone +49 6078 9385 813 · sales.central@infoguard.com
Middle East	InfoGuard Representative Office Dubai · Phone +971 50 255 1533 · sales.middleeast@infoguard.com