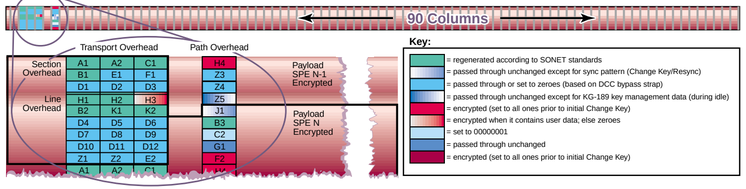
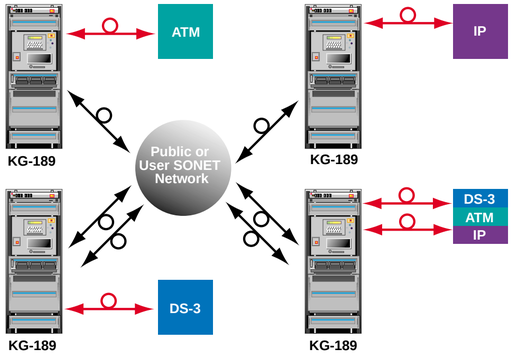
KG-189 AND SONET — ASSURED THROUGHPUT AND SECURITY



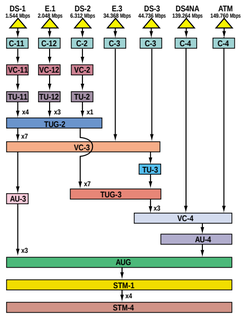
SONET NETWORK



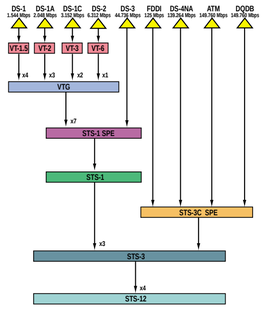
HOW IT WORKS

KG-189 operates between the SONET multiplexer/demultiplexer and the network node to provide transparent encryption of high data rate communications. 1 to 12 full-time SONET links provide data routing with full traffic flow security. Denial of communications intelligence is complete.

SYNCHRONOUS DIGITAL HIERARCHY - SDH



SYNCHRONOUS OPTICAL NETWORK - SONET



Characteristic	Non-Redundant Configuration	Redundant Configuration
Height	23 in. Newton/24 in. EIA-STD rack	23 in. Newton/24 in. EIA-STD rack
OC-3/OC-12	28 in. (70 cm.)	28 in. (70 cm.)
OC-48* (19 in. rack mountable)	17.5 in. (44.5 cm.)	17.5 in. (44.5 cm.)
Weight		
OC-3/OC-12	55 lbs. (25 kg.)	75 lbs. (34 kg.)
OC-48*	60 lbs. (27 kg.)	70 lbs. (32 kg.)
Primary Power		
OC-3/OC-12	-40 to -60 Vdc, 150W max @ -48Vdc	-40 to -60 Vdc, 250W max @ -48Vdc
OC-48*	-40 to -60 Vdc, 300W max @ -48Vdc	-40 to -60 Vdc, 540W max @ -48Vdc
Backup Power		
Operational	-40 to -60 Vdc (from PBX backup source)	-40 to -60 Vdc (from PBX backup source)
Memory	Battery (standard 9V alkaline)	Battery (standard 9V alkaline)
SONET Interface (conforms to Bellcore TR-253. Issue 2)		
OC-3	Long Reach	Long Reach
OC-12	Intermediate, Long Reach	Intermediate, Long Reach
OC-48*	Short Reach	Short Reach
Connectors	ST (also SC, FC with optional connector conversion kit)	ST (also SC, FC with optional connector conversion kit)
Optical Fiber	Single mode	Single mode
Key Management Interface		
Benign Fill	DS-101	DS-101
Red OVS	KSD-64	KSD-64
Control Interface		
Local	Front panel and LED display	Front panel and LED display
Remote	RS-232 or Ethernet	RS-232 or Ethernet
Remote Signal Control	De-bounced TTL	De-bounced TTL
Card Set		
OC-3	OC-3 Tx/Rx (2)	OC-3 Tx/Rx (4)
	Encryption Module (EM) (1)	EM (1)
	Control Processor/Key Processor (CP/KP) (1)	CP/KP (1)
	External Synchronous Interface (ESI) (1)	ESI (1)
OC-12	OC-12 Tx/Rx (2)	OC-12 Tx/Rx (4)
	EM (1)	EM (1)
	CP/KP (1)	CP/KP (1)
	ESI (1)	ESI (1)
OC-48*	OC-48 T/R (2)	OC-48 T/R (4)
	EM (2)	EM (4)
	Control Module (1)	CM (1)
	ESI (1)	ESI (2)
Equipment Availability		
OC-3/OC-12	99.99957%	99.99980%
OC-48*	99.99964%	99.99992%
Maintainability		
Mean Time Between System Failures	>5 years	>11 years
Service Interruption or Degradation	< 12 minutes (all data paths)	< 12 minutes (unprotected data path)
		< 7 seconds (protected data path)
Mean Time To Repair	< 30 minutes	< 30 minutes
Mean Time To Service Restoral=		
Protected traffic path failure	N/A	< 7 seconds
Unprotected traffic path failure	< 12 minutes (all data paths)	< 12 minutes (encryption module)
Non-data path failure	0 seconds (CP/KP, ESI)	0 seconds (CP/KP, ESI, Standby Optics)

*OC-48 configuration currently in development, specifications subject to change. ** Bellcore TR-253 specifies extended, long, intermediate and short reach characteristics for SONET equipment. Where not otherwise specified, intermediate and short reach requirements are met through the use of optical attenuators (provided). ‡Repair of all failed modules can be accomplished without power interruptions. In the redundant configuration, most failures can be repaired without service interruption. In either configuration, service is automatically restored on replacing the failed module.

Motorola
Information Systems & Security Products Division
8220 E. Roosevelt Street, M/D R-1204
P.O. Box 9040, Scottsdale, AZ 85257
Telephone: (480) 441-5443 Fax: (480) 441-0843
Web: http://kg-189.motorola.com
E-mail: kg189@motorola.com

RC-115-4003

MOTOROLA

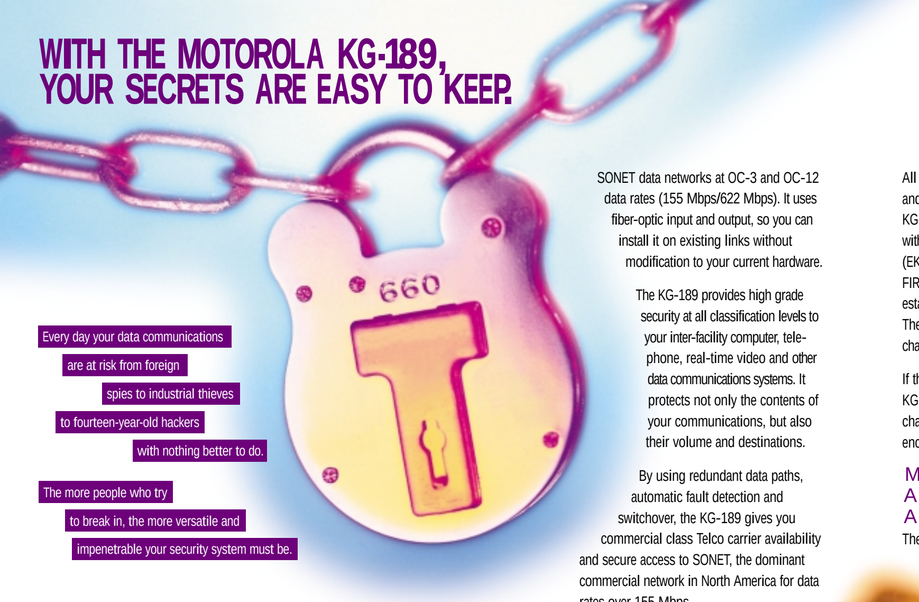
Secure Voice, Data, Network and Key Management

THE MOTOROLA KG-189.

IT KNOWS HOW TO KEEP A SECRET.

MOTOROLA

WITH THE MOTOROLA KG-189, YOUR SECRETS ARE EASY TO KEEP.



Every day your data communications
are at risk from foreign
spies to industrial thieves
to fourteen-year-old hackers
with nothing better to do.

The more people who try
to break in, the more versatile and
impenetrable your security system must be.

The threats to keeping your communications secure are quite real and may be a matter of national security. That's why you need a system to provide Type I security protection. And it's got to be easy and seamless. The Motorola KG-189 does ***both*** through:

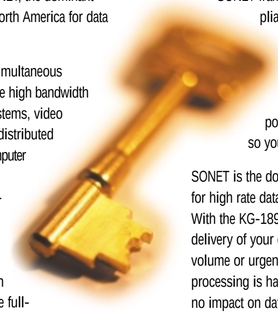
- ***Telco-class availability*** – we have designed in redundant optical interfaces, Automatic Protection Switching (APS) and Hitless key changes for high availability (>99.9998%).
- ***Remote status and control*** – without requiring special workstations! We include Java™ Graphical User Interface software. Together with an inexpensive Ethernet proxy, the KG-189 allows access to your existing Windows®- or UNIX®-based computer assets. SNMP monitoring and control are also supported via your SNMP manager facilities, such as the HP® OpenView® system.
- ***Traffic flow security*** – for all types of payload data, packetized or connection-based (*e.g.*, IP, ATM, FDDI, DS-1,2,3 or 4, DQDB MAN, B-ISDN).
- ***Scalable architecture/bandwidth flexibility*** – both OC-3 and 12 (155/622 Mbps) models are available right now. And the substantially faster and smaller OC-48 (2.5 Gbps) is currently under development with field tests available 4Q00 and production units available 3Q01. OC-192 (10 Gbps) will follow OC-48.

THE MOTOROLA KG-189 TRUNK ENCRYPTOR

The Motorola KG-189 high-capacity trunk encryptor is designed to operate within SONET data networks at OC-3 and OC-12 data rates (155 Mbps/622 Mbps). It uses fiber-optic input and output, so you can install it on existing links without modification to your current hardware.

The KG-189 provides high grade security at all classification levels to your inter-facility computer, telephone, real-time video and other data communications systems. It protects not only the contents of your communications, but also their volume and destinations.

By using redundant data paths, automatic fault detection and switchover, the KG-189 gives you commercial class Telco carrier availability and secure access to SONET, the dominant commercial network in North America for data rates over 155 Mbps.



The KG-189 allows for simultaneous encryption across multiple high bandwidth sources such as PBX systems, video teleconferencing, LANs, distributed simulations, dedicated computer networks and real-time imagery distribution centers. That means you can use a single encryption node to meet all of your data protection needs, from one to twelve full-time links—all with complete confidentiality.

EASY NETWORK MANAGEMENT

We've designed the Motorola KG-189 so it's easy to use. Just turn it on, make a few simple configuration selections and load the initial key. That's all there is to it.

All selections are located on the front panel and can be operated remotely via the unique KG-189 Java GUI. Plus, the KG-189 interfaces with NSA's Electronic Key Management System (EKMS) for the initial key load and uses the FIREFLY public key algorithm to automatically establish encryption keys between encryptors. The KG-189 automatically negotiates daily key changes between units, with no traffic data loss.

If there's ever a loss of communication, your KG-189s automatically switch to a spare channel, immediately re-establishing the encrypted session with minimal loss of data.

MOTOROLA KG-189 AND SONET: A SECRET ALLIANCE

The KG-189 uses the Z5 (N1) field of the SONET frame header and SONET-compliant COTS components for all TELCO functions, complementing the Motorola COMSEC subsystems. There's no need to reserve a portion of the user data frame—so you get full SONET capacity.

SONET is the dominant commercial option for high rate data communications today. With the KG-189 and subscription to SONET, delivery of your data is assured, even when volume or urgency is high. All security processing is handled automatically, with no impact on data rate. All—as in, 100%—of the SONET bandwidth is available for transmitting your data.

EASY TO MAINTAIN

Should something go wrong with the KG-189, self-diagonstics isolate and display the problem on the front panel and an LED lights up on the failed board. This makes replacing modules a breeze. Repairs typically take less than 12 minutes—with no system data interruption.

Of course, the KG-189 is backed by Motorola. Not only will we help you install your system and train your personnel, we also provide a full two-year warranty.

So if data encryption is vital to your success, call your Motorola representative today. Make the KG-189 the best-kept secret you'll ever have.

For technical assistance or more information, please call 480-441-5443 or visit our Website: http://kg-189.motorola.com

KG-189 PRODUCT SPECIFICATIONS

Transport Overhead Bytes	Contents	KG-189 Handling
A1, A2	Framing bytes	Generated by transmit optics card.
C1	Section trace (formerly STS-1 ID)	Controlled by transmit optics card
B1	Section BIP-8, parity over the STS-N frame after scrambling	Generated by transmit optics card.
E1, E2, F1, D1-D12, Z1 (S1), Z2 (M2)	Transport data communication channel	Passed through or set to zeroes based on the DCC bypass strap.
H1, H2	Payload pointer	Processed as specified in TR-253 for Line Terminating Equipment.
H3	Pointer action byte	Processed per TR-253. Encrypted when it contains user data; filled with zeroes when it does not.
B2	Line BIP-8, parity over the STS-1 line OH and SPE	Generated by transmit optics card.
K1, K2	Automatic Protection Switching Channel	Generated by transmit optics card
Path Overhead Bytes*		
J1	STS path trace	Passed unchanged except for 8 byte KG-189 synchronization flag sent during Resync or Change Key operation.
B3	Path BIP-8, parity over STS-1 or STS-Nc SPE	Offset such that path parity is preserved through the KG-189.
C2	STS path signal label	Set to 00000001 (equipped - non specific payload)
G1	Path status	Passed unchanged
F2	Path user channel	Encrypted; prior to first Change Key operation, set to all ones.
H4	Indicator byte	Encrypted; prior to first Change Key operation, set to all ones.Also used (read only) to perform KG-189 autosync.
Z3, Z4	Growth bytes	Blocked or bypassed based on the DCC bypass strap.
Z5 (N1)	Tandem connection	Normally passed unchanged. When channel is idle, bits 5-8 may be used for key management functions.

*Note: POH handling overridden when Path AIS or Line AIS received or KG-189 critical alarm triggered; output POH then set to all ones(per SONET standard). The descriptions above explain the normal handling of the POH bytes.