KG-81, KG-94/A, KG-95-/1/2/R, KG-194/A

The KG-94 and KG-194 are part of the WALBURN family of full duplex, high-speed key generators that provide encryption of digital traffic. KG-194 is essentially a KG-94 with added features. These devices provide full duplex/simplex encryption for all classification levels and are crypto graphically compatible and interpretable (within their respective data rates). Applications include microwave trunks, high speed landline circuits, video teleconferencing, and T-1 satellite channels.

The KG-94 and KG-194 are tactical versions of the KG-94A and KG-194A. The KG-194 is an upgraded version of the KG-94 design. All versions are cryptographically compatible with each other, as well as with the KG-81 and KG-95 within their respective data rates in the traditional key mode. When used in conjunction with the Interface Adapter Unit, they can be a direct replacement for the KG-27. The KG-194 and 194A are interoperable only with other KG-194(A) in the FIREFLY mode. The KG-94 and KG-194 family functions with MIL-STD 118/114, RS-422 and RS-449 standard synchronous interfaces. Encryption and decryption takes place at speeds of 9.6 Kbps to 13 Mbps. The KG-194 and 194A generators are compatible with FIREFLY remote re-keying and can also be keyed with the KSD-64A. Traditional keying is accomplished with the KOI-18, KYK-13, KYK-15, KOK-12, and the Data Transfer Device (AN/CYZ-10) for any of the KG-94s and 194s. The KG-94 and 194 families may be used with fix plant and tactical trunk encryption devices. They are approved for use at all classification levels up to TOP SECRET. They are UNCLASSIFIED controlled cryptographic items (CCIs) when unkeyed.

KG-81: Provides full-duplex encryption of digital trunks. It is rack mounted using the HNF-81-1/2 interconnect housing frame. The KG-81 is used primarily at major communications stations for bulk data and video encryption.

KG-94: Provides emerging low and medium tactical and non tactical digital trunk encryption. It is rack mounted using the HNF-81-1/2 interconnect housing frame and supports the Joint Tactical Communications program in association with Marine Corps AN/TTC-42 and AN/TRC-170 switches.

KG-94 equipment

KG-94A: Is an environmentally repackaged, ruggedized version of the KG-94 that supports the Marine Corps unit level circuit switches (SB-3865) and the Digital Wideband Transmission System (DWTS).

KG-194: Is a less costly version of the KG-94 that incorporates a remote keying capability and implements FIREFLY technology. The KG-194 is used for digital and voice bulk encryption at major communications stations.

KG-194A: Is a less costly ruggedized version of the KG-194. It satisfies the same basic requirements as the KG-94A, incorporates a remote keying capability, and implements FIREFLY technology.

KG-95: Is a general-purpose, high-speed, full-duplex, fixed-plant, key-generating encryption device used for video, data links, missile test range communications. There are three KG-95 equipment configurations. The KG-95-1 is a general purpose version of the KG-95, capable of operating at any data rate between 10 and 50 Mbps. It is compatible with the KG-81, KG-94/94A, 194/194A over their common data rates and when using traditional key. The KG-95-2 operates only at the fixed DS-3 data rate of 44.736 Mbps. It is fully compliant with ANSI T1.102-1987 for DS-3 transmission and reception. The KG-95R is two KG-95-2s in a dual frame. The frame provides for hot spare capability. Other capabilities include remote operation, remote status check, and remote over-the-air rekey exchange, in addition to new key management techniques and a fiber optics interface. The KG-95R is a composite of two KG-95-2s in a redundant configuration.

The KG-95 configurations have a MIL-STD 118/114 interface. All three equipment configurations are capable of operating form traditional, punched paper key or Remote Rekey Keying (RRK) material. Traditional key may be loaded via a KOI-18, KYK-13, KYK-15, or Data Transfer Device. Remote Rekey Keying (RRK) material is loaded via a KSD-64 or the Data Transfer Device and offers the user a one-year crypto period. When using RRK material, the operator must instruct the KG-95 to perform a change key operation once every twenty-four hour period. The daily operations required under traditional key and RRK material need to be initiated at one end of the link through the equipment's front panel or rear panel remote command lines. During traditional keying traffic, down time for a change key command is approximately 500 milliseconds. The down time during RRK is 30 seconds. The KG-95-1 operates at 10-50 Mbps. The KG-95R operates at the DS-3 rate of 44.376 Mbps.

These systems are approved for use at all classification levels. The manufacturer is Motorola Secure Telecommunications, Scottsdale, Arizona. Cost will depend on the size of the production run. Unit cost of previous production run was $7,950 for a KG-95-2 and $16,000 for KG-95R.

KIV-19: Is a miniaturized KG-194 that is functionally equivalent and interoperable with the KG-194 and KG-194A. The KIV-19 is not intended to replace the KG-194 and KG-194A but to fill new requirements and unique backfit requirements that have strict size and weight constraints. The KIV-19 is certified to secure all classification levels and categories. It is an UNCLASSIFIED controlled cryptographic item (CCI) when unkeyed. When keyed, the equipment carries a classification equal to that of the key installed.

HNF-81-1: Is approved for all levels of classified traffic and is designed to have one or two KG-81, KG-94, or KG-194 cryptographic devices. The terminal blocks in the rear of the HNF-81-1 provide connections between the input or output cabling and the connectors.

HNF-81-2: Is approved only for the transmission of unclassified or previously encrypted traffic unless it is transmitting bypassed information with prior approval of National Security Agency (NSA). The HNF-81-2 is mechanically similar to the HNF-81-1 except the terminal blocks in the rear of the frame are mounted on printed wiring boards giving the user cryptographic bypass ability.