KNG Encryption Overview

RELM KNG Series radios are available with optional encryption features to support secure tactical communication. Implementing standards based encryption protocols as defined in TIA-102.AAAD Block Encryption Protocol assures interoperability. RELM radios with encryption have been validated to the National Institute of Standards (NIST) FIPS-140-2 program, providing assurance that encryption services are implemented in a secure and meaningful way.

Encryption Algorithms - RELM provides both Advanced Encryption Standard (AES) 256 bit key length encryption as well as Data Encryption Standard (DES) 56 bit key length encryption. In general, encryption keys of less than 128 bits are no longer considered to be secure. US Federal government agencies were required to transition to AES by May 2007. Availability of DES operation remains important to enable interoperability with legacy systems. While DES operation does provide a level of privacy from casual listeners, it should not be considered secure.

Encryption Keysets – KNG Series radios currently support two keysets of up to 32 keys each. Keys can be either DES or AES.

Encryption Keyloading - RELM KNG Series radios are compatible with the Project 25 Encryption Keyload Standard. Any key loading device that implements this standard can be used to load KNG radios utilizing RELM keyload cables. KNG Series radios have been proven compatible with the KVL-3000+ series keyload devices.

Encrypted Operation - Conventional channels or trunked talk groups can be programmed for clear only, user selectable clear/encrypted or encrypted only. If the channel is configured as selectable, customer programming software is used to program the clear/secure activation key. Customer programming software links the channel/talk group with a predefined (default) key. For conventional channels, the key picklist function can be used to select a different key for transmit. For receive operation, the radio will automatically select the correct key provided it is available in the radio.

Manual Key Management - KNG Series implement infinite key retention which preserves encryption keys in the event of power loss to the radio unit. KNG Series radios provide for a programmable function key which allows all keys in the radio unit to be deleted or zeroized. Encryption keys may also be deleted using a keyload device.

Over the Air Rekey - KNG Series radios are also compatible with Project 25 Standards for Over-the-Air Rekeying (OTAR). This option allows for an infrastructure system to maintain encryption keys in a KNG Series radio. Once an initial encryption key configuration has been downloaded to the radio, an OTAR system can manage encryption keys wirelessly without physical contact with the radio. Management of keys can include downloading new keys or deleting existing keys in the radio. This option supports best practice for secure operation.

RELM Wireless Corporation
7100 Technology Drive
West Melbourne, FL 32904
800-821-2900 / sales@relm.com
www.relm.com

KNG Encryption Overview

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. **1185**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

FIPSCOM Cryptographic Module *by* RELM Wireless Corporation

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

FIPSCOM Cryptographic Module *by* RELM Wireless Corporation
(Hardware Versions: P/N 7011-30967-000, Versions 042009[1] and 042109[2]; Firmware Versions: 0722-05072-000[1] and 0722-05072-001[2] (bootcodes) and 0722-05073-003[1,2] (application); Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: *InfoGard Laboratories, Inc., NVLAP Lab Code 100432-0*
is as follows: *CRYPTIK Version 7.0*

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: (Multi-Chip Embedded)	Level 1	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level N/A	*tested in the following configuration(s):*	N/A

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #899); RSA (Cert. #139); SHS (Cert. #462)**

The cryptographic module also contains the following non-FIPS approved algorithms: **DES; AES (AES Cert. #899, key wrapping; key establishment methodology provides 256 bits of encryption strength)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: _____

Dated: Sep 21, 2009

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: September 9, 2009

Director, Industry Program Group
Communications Security Establishment Canada

RELM Wireless Corporation
7100 Technology Drive
West Melbourne, FL 32904
800-821-2900 / sales@relm.com
www.relm.com