

Version
01.00October
2004

R&S® KGE 3000

Key generation and encryption module

- ◆ Hardware-based true random number generator
- ◆ Encryption of keys by symmetric algorithms
- ◆ Internal built-in tests
- ◆ PC communication via USB 1.1

Integral part of Rohde & Schwarz management system

The R&S® KGE 3000 Key Generation & Encryption Module is a module for the generation and encryption of keys. It has been optimized for the R&S® RNMS 3000 and R&S®SMS 3000 management systems. The module should be operated in combination with one of these Rohde & Schwarz management systems to administer and distribute symmetric keys. The functionality of the R&S®KGE 3000 can be integrated in any other appropriate Rohde & Schwarz management system.

The main features of the R&S®KGE 3000 are the following:

- ◆ Generation of keys by the internal hardware-based true random number generator
- ◆ Provision of encrypted (black) keys for the R&S®M3TR and R&S®MMC 3000, including the container structures
- ◆ Encryption of external keying material

The communication with the management system PC, or a USB-compatible device, is via the USB 1.1 interface.

Hardware-based true random number generator

One of the primary tasks of the R&S®KGE 3000 is the generation of random numbers. The module integrates a true random number generator based on a hardware noise generator. Several tests ensure the quality of the random bit stream generated. Mathematical post-processing is performed to produce random numbers of high statistical quality.

Key encryption using symmetric algorithms

The R&S®KGE 3000 provides high-quality, high-capacity symmetric algorithms for the encryption of keys and keying material. The encryption algorithms can be customized to accommodate individual user requirements.

The R&S®KGE 3000 supports black key management, i.e. the keys are encrypted after they have been generated and built into the key container structures of the R&S®M3TR or R&S®MMC 3000. The keys are provided by the R&S®KGE 3000 only in an encrypted (black) state. Besides protecting the keys' confidentiality by encryption, additional measures ensure their integrity and authenticity.

In addition to these functions, keying material (e.g. key files) can be encrypted by the R&S®KGE 3000.

Specifications

Dimensions (H × W × D)	35 mm × 105 mm × 160 mm
Power supply	5 V / <100 mA (via USB 1.1 interface)
Operating temperature range	+5 °C to +40 °C
Storage temperature range	-40 °C to +70 °C

Ordering information

Type	Order No.
R&S®KGE 3000	3554.7707
Included in delivery	R&S®KGE 3000 Drivers for Windows 2000 / XP USB A-B cable

Internal built-in tests

Internal built-in tests, particularly for the random number generator, are performed by the R&S®KGE 3000. The module will be deactivated if any of the built-in tests fails and all requests using the random number generator will be rejected.

Thorough statistical tests are applied after device start-up in order to detect any failure in the physical noise source. The R&S®KGE 3000 will only change to the operating mode after the tests have been carried out successfully. Continuous runtime tests are performed to ensure that the random number generator works correctly and that only random numbers of high statistical quality are accepted and used.



www.sit.rohde-schwarz.com

Customer Support: Telephone: +49 30 65884111 · Fax: +49 30 65884184 · E-mail: support@sit.rohde-schwarz.com