R&S®KGE3000 Key Generation Equipment

True random data for security management applications

ROHDE&SCHWARZ

Secure Communications

Product Brochure | 03.00

R&S®KGE3000 Key Generation Equipment

At a glance

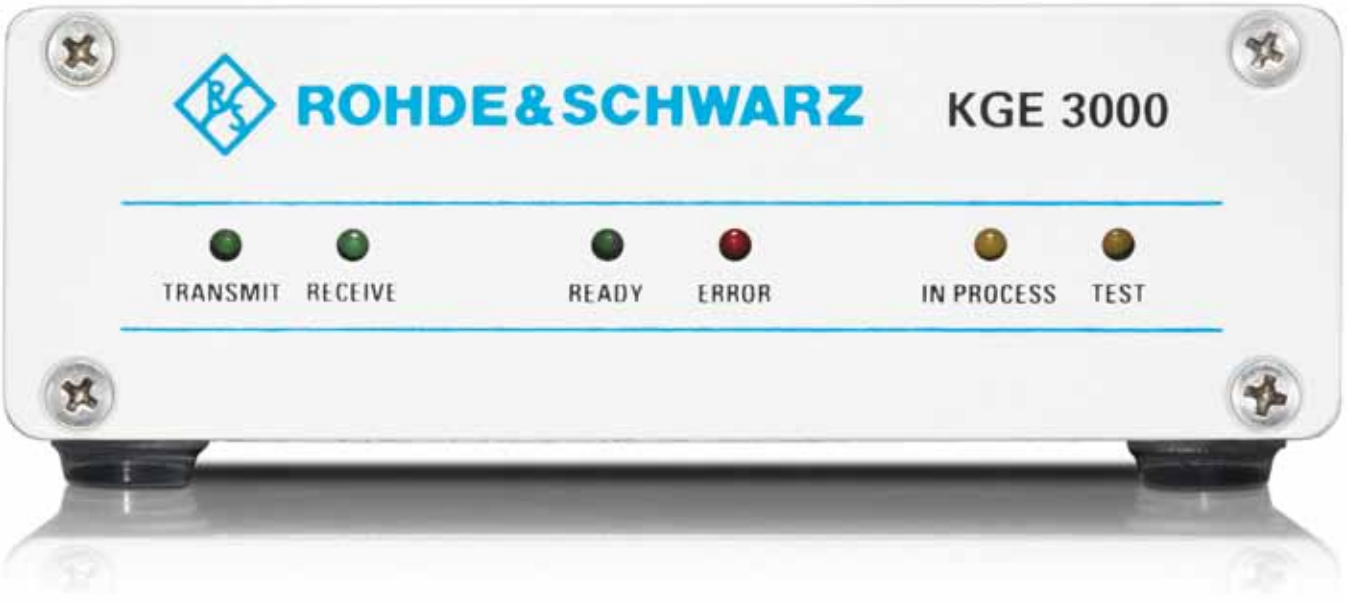
The R&S®KGE3000 hardware-based true random number generator delivers output optimized to the specific requirements of Rohde&Schwarz security management applications.

Security management systems require a reliable source of dedicated and qualified input data to generate and distribute sensitive information within a network. The different R&S®KGE3000 models use encryption to protect the confidentiality of the keys and provide additional measures to continuously ensure the integrity and authenticity of the keying material.

The R&S®KGE3000 is a true random number generator (TRNG) that uses two independent physical entropy sources. The data is postprocessed to produce random numbers of high statistical quality. The input for the high-capacity symmetric algorithms for key containers, keys and keying material is delivered to the application in the management system PC over a USB interface. Built-in tests (BITs) continuously monitor the quality of the output of the TRNG material. The output of the TRNG has been tested according to stringent evaluation methodology (AIS31 PTG.2) and comprehensive statistical test suites (NIST SP 800-22, DIEHARD). The design ensures that no sensitive data (e.g. keys) is stored within the device itself.

Key facts

- True (physical) random number generator
- Design and implementation optimized for Rohde&Schwarz security management systems
- State-of-the art security mechanisms (algorithms, authentication, encryption, integrity)
- Internal built-in test (BIT) for quality control
- Tested to NIST SP 800-22, DIEHARD and AIS31 PTG.2



R&S®KGE3000 Key Generation Equipment

Benefits and key features

High quality keying material through robust testing and careful design

- High quality entropy sources ensure compliance to exacting standards
- Continuous tests constantly check adherence to quality requirements
- Separate inputs, amplifiers, filters, converters, microcontrollers and postprocessing eliminate any negative external and internal influences

▷ page 4

Optimal fit to application requirements due to flexible structure

- Seamless integration into target application eliminates risk of operator-induced error
- Options provide customized solutions
- Assembling unique customer-defined parameters for waveform security
- Flexible use of different roles, needs and functions while retaining the security level

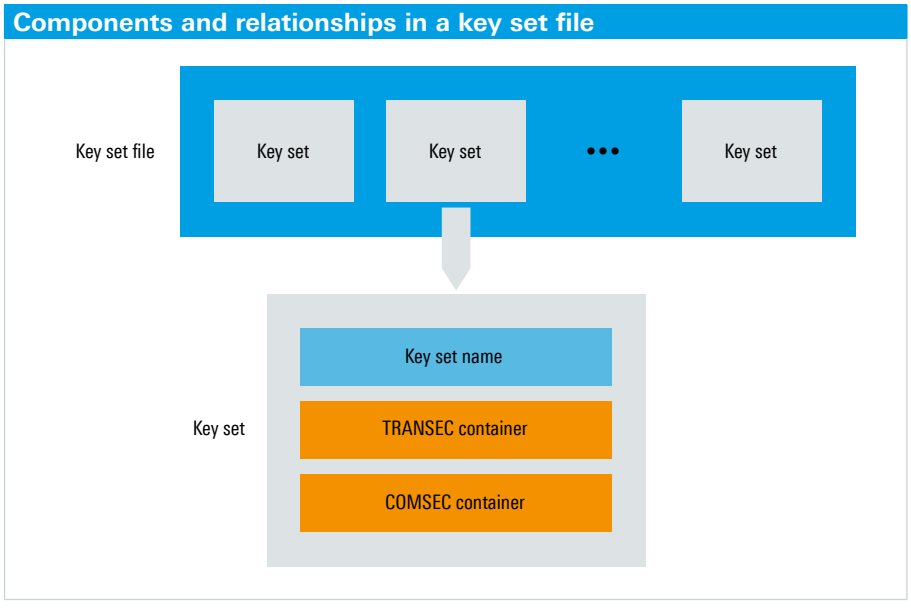
▷ page 5

Security features enhance the integrity of the management application

- No storing of critical “red” data in the device makes the system less vulnerable
- Key protection key (KPK) wraps sensitive keying material (key container) for secure distribution throughout the system

▷ page 6

Components and relationships in a key set file



The R&S®KGE3000 models for Rohde&Schwarz radios provide an encrypted key set file with a user-defined number of key sets for the R&S®RNMS3000 mission planner application.

High quality keying material through robust testing and careful design

High quality entropy sources ensure compliance to exacting standards

Two separate and independent physical sources provide the raw data for the random numbers. The raw data test is based on the German national requirements for physical randomness (AIS31 PTG.2). The output data is subjected to the NIST SP 800-22 and DIEHARD test suites. The mathematical postprocessing uses AES-256 with CBC-MAC.

Continuous tests constantly check adherence to quality requirements

A statistical test is carried out on the quality of the digitized physical signals (raw data) at the source each time the device is turned on. This ensures that the quality of the physical source has not degenerated beyond an acceptable level. The device will only switch to the operating mode when the test has been passed successfully. During operation, continuous runtime tests are carried out to evaluate the level of entropy of the input. Any violation of the boundaries will result in the device ceasing to operate.

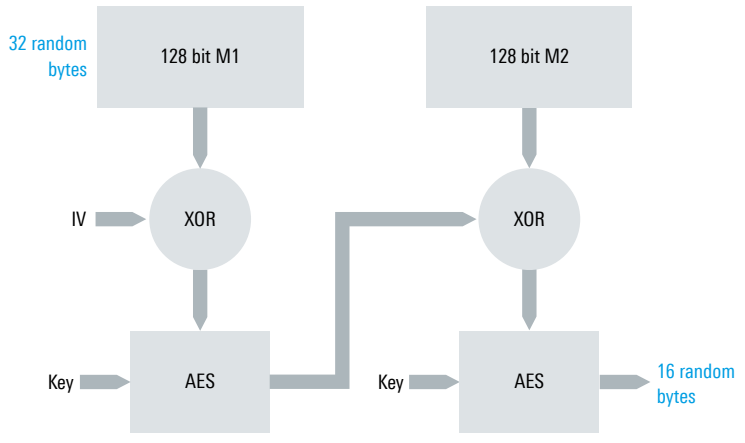
Separate inputs, amplifiers, filters, converters, microcontrollers and postprocessing eliminate any negative external and internal influences

Two independent Z diodes each generate a separate noise signal. These signals are fed into the input of the differential amplifier to produce a differential noise signal. The differential amplifier suppresses periodic disturbances, such as fluctuation in the supply voltage from the Z diodes. The inverted output is fed back over a low-pass filter to the input of the differential amplifier to determine the working point of the two differential receivers.

The signal is digitized by connecting the non-inverted output of the differential amplifier to the input of an inverting A/D converter. The A/D converter is implemented as a Schmitt trigger. The random digital signal emitted by the converter is fed back over a low pass filter to determine the working point of the Schmitt trigger.

A microcontroller combines all random digital signals in groups of three to a bitwise XOR. The resulting bits are written to a byte buffer. All 32 random bytes from the byte buffer are processed using AES-256 with CBC-MAC with a fixed key and initialization vector (IV) to produce the 16 random bytes.

Flow diagram of the postprocessing



Optimal fit to application requirements due to flexible structure

Seamless integration into target application elimates risk of operator-induced error

The R&S®KGE3000, with its intuitive user interface, is closely integrated into the R&S®RNMS3000 and R&S®SMS3000 management systems, eliminating a primary source of degraded security variables: human intervention. A click on the field in the management application launches the process, which is carried out to its conclusion without any further user input.

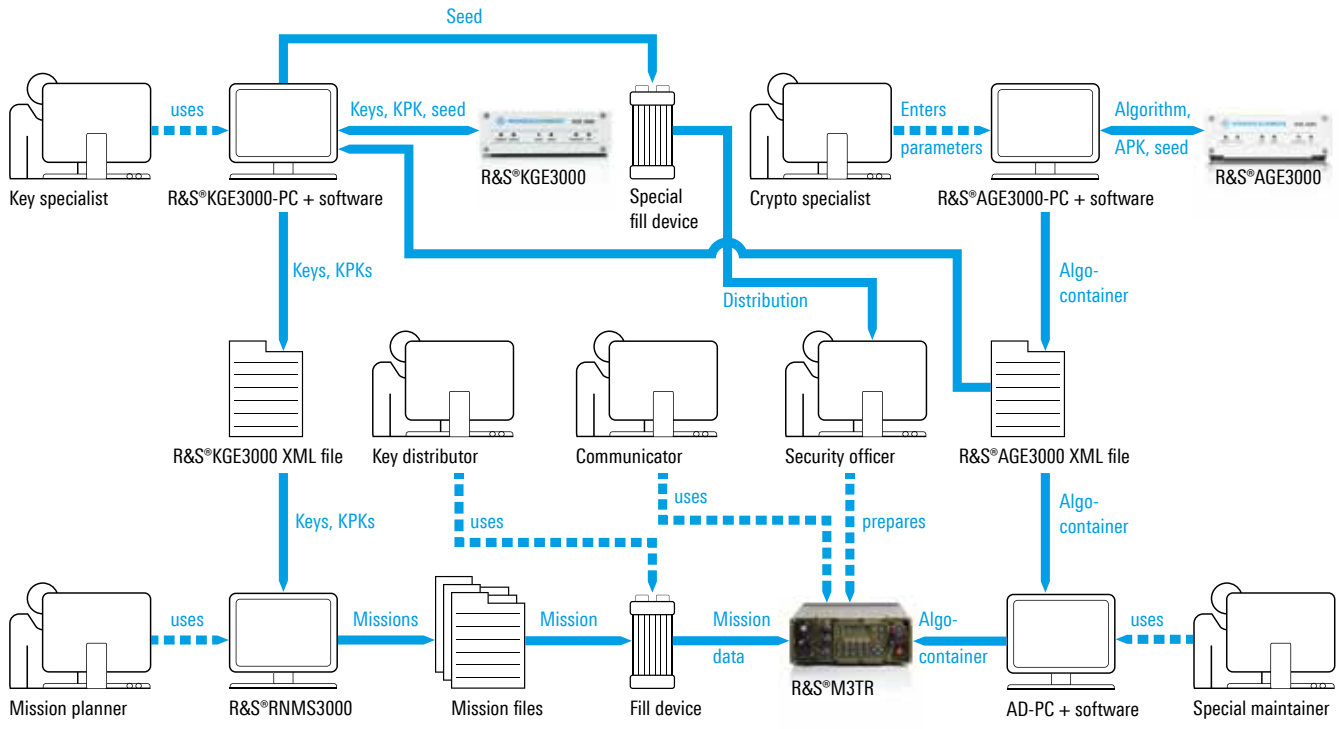
Options provide customized solutions

The R&S®KGE3000 provides the exact data format specified by the application/algorithm. The different requirements for data containers, key structures, and input for initialization vectors, key pairs, proprietary and standard (e.g. AES) algorithms allow for customized solutions. The ability to adjust and adapt numerous variables supports customer-specific solutions for key infrastructures.

Assembling unique customer-defined parameters for waveform security

The R&S®AGE3000 provides the necessary input to customize RSCA-2G waveforms, i.e. R&S®SECOM-H, R&S®SECOM-V, SDV (Secure Digital Voice) and Secure xDL. A special model of the R&S®KGE3000 (R&S®KGE3000 RSCA-2G) is also available to provide the necessary key data for a system customized by the R&S®AGE3000.

Flexible use of different roles, needs and functions while retaining the security level



The R&S®KGE3000 and the the R&S®AGE3000 are used in combination to secure a highly complex, role-based critical key management infrastructure.

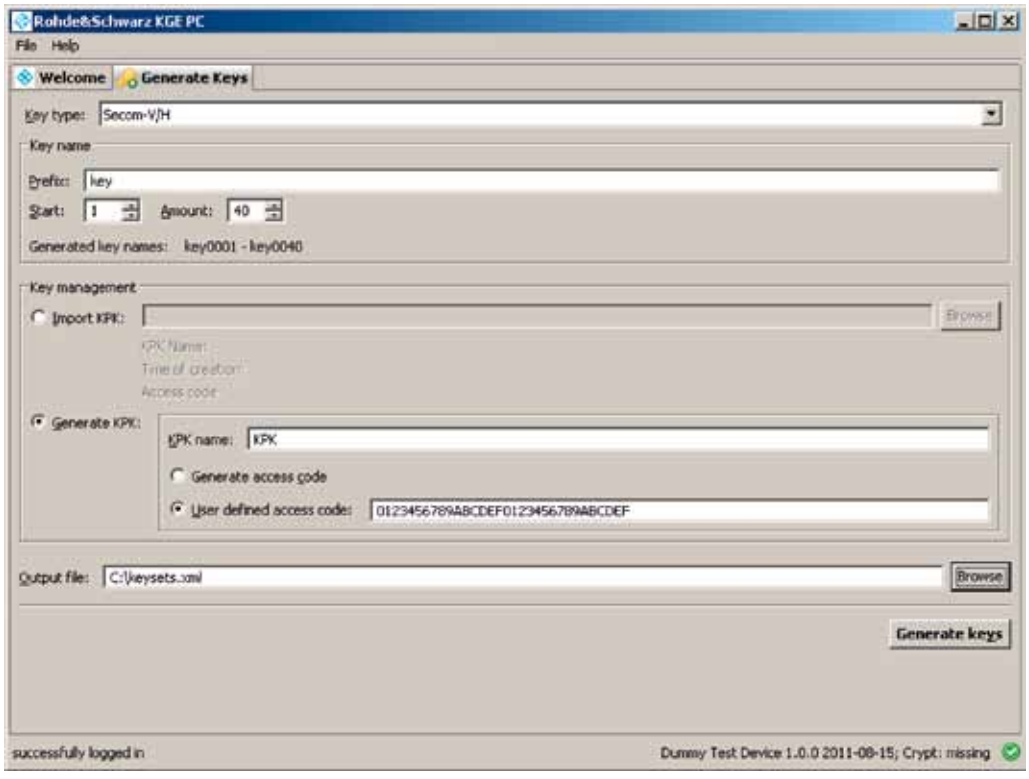
Security features enhance the integrity of the management application

No storing of critical “red” data in the device makes the system less vulnerable

The R&S®KGE3000 processes the information/commands it receives from the application. Keying material in plain form is not stored within the device itself. This reduces the number of instances where “red” keying material is present to a minimum. Standard security measures include PIN access, active and passive exclusive device allocations to specific applications and/or customer versions and non-legible processors protecting data and information within the device.

Key protection key (KPK) wraps sensitive keying material (key container) for secure distribution throughout the system

Critical keying material is transmitted as a key container within the system. The KPK generated by the KGE, encrypts the plain key and places it in a wrapper within the key container. The wrapper consists of the key and a MAC. The MAC is calculated using the key ID and the key.



KGE software PC interface for R&S®KGE3000.

Specifications

Specifications		
Power supply	voltage	5 V, < 100 mA (via USB 2.0 interface)
Interface		USB 2.0
USB cable	length	1.5 m
Environmental data		
Operating temperature range		+5 °C to +40 °C
Storage temperature range		–40 °C to +70 °C
Dimensions	W × H × D	105 mm × 35 mm × 160 mm (4.1 in × 1.4 in × 6.3 in)
Weight		approx. 550 g (1.2 lb)

Ordering information

Designation	Type	Target system	Order No.
Key Generation Equipment	R&S®KGE3000	R&S®SMS3000 for R&S®MMC3000	3554.7707.02
	R&S®KGE3000 RSCA-1G	R&S®RNMS3000 for R&S®SECOM-H/R&S®SECOM-V/ R&S®SECOM-P and SDV and Secure xDL	3554.7707.06
	R&S®KGE3000 RSCA-2G	R&S®RNMS3000 for R&S®SECOM-H/R&S®SECOM-V/ R&S®SECOM-P and SDV and Secure xDL	3554.7707.07
Algorithm Generation Equipment	R&S®AGE3000 RSCA-2G	R&S®RNMS3000 for R&S®SECOM-H/R&S®SECOM-V/ R&S®SECOM-P and SDV and Secure xDL	3554.7707.08

Service you can rely on

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability

Certified Quality System
ISO 9001

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin
Phone +49 30 65884-223 | Fax +49 30 65884-184
E-mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com
Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

Regional contact

- Europe, Africa, Middle East | +49 89 4129 12345
  customersupport@rohde-schwarz.com
- North America | 1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latin America | +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacific | +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com
- China | +86 800 810 8228/+86 400 650 5896
  customersupport.china@rohde-schwarz.com

PD 0758.1764.12 | Version 03.00 | June 2012 | R&S®KGE3000

0758176412