R&S®MMC3000
MULTIMODE MULTIROLE CRYPTO DEVICE

Ruggedized HF/VHF/UHF and SatCom security for voice and data

Product Brochure
Version 05.00

ROHDE&SCHWARZ
Make ideas real

AT A GLANCE

The R&S®MMC3000 is a fully ruggedized tactical crypto device used to encrypt and decrypt voice and data communications at the highest security levels. TEMPEST-proof, it is interoperable with HF/VHF/UHF radio, satellite communications and line transmission equipment. It is perfectly suited for deployment on stationary and mobile platforms in rugged terrain and in naval and airborne environments.

The R&S®MMC3000 is based on the ELCRODAT 4-2. The ELCRODAT 4-2 is approved for communications up to NATO COSMIC TOP SECRET. It has been a proven key component in the field of highly secure communications and helps safeguard interoperability between NATO nations. The R&S®MMC3000 does not contain NATO crypto algorithms but complies with the high standards regarding robustness, flexibility and security.

The R&S®MMC3000 device supports simplex, half-duplex and duplex modes to satisfy the requirements of the widest range of digital and analog applications for both local and remote operation.

The R&S®MMC3000 can be operated either with a control unit or the MIL-bus module. A customizable crypto algorithm provides the uniqueness and exclusivity needed for different national and coalition scenarios.

In data crypto mode, the device is seamlessly integrated into data transmission systems equipped with standard military interfaces (most standard military interfaces are supported). The vocoder used in voice mode optimizes speech clarity even in noisy transmissions. The flexible and future-ready design includes a protected software download process and a slot for an additional crypto board for upgrading the device to meet future requirements.

The R&S®MMC3000 has a wide range of accessories to integrate the device in complex communications infrastructures. A security management system (R&S®SMS3000) is augmented by a data loading device (DLD), mounting frame, power supply unit and components for the remote operation of the control unit.

Key facts

- Voice and data encryption to the highest security levels
- Protects HF/VHF/UHF, satellite communications and line transmission
- Fully rugged, tamper protected, TEMPEST-proof
- Stationary and mobile deployment in all military branches (army, navy, air force)
- Customizable crypto algorithms for specific user requirements

BENEFITS AND KEY FEATURES

Dedicated operator interfaces for various applications

- Remote control software systems management interface
- MIL-bus communications systems management interface
- Control unit user interface
- Headset/intercom interface
- page 4

Comprehensive protection through elaborate security concept

- Audited production environment
- Hardware red-black separation and tamper protection
- Secure key generation and management
- page 6

Versatility through multiple traffic/operating modes and transmission methods

- Traffic modes according to operating modes and transmission methods
- Operating modes for voice and data transmissions
- Teletype for extremely reliable communications
- Ready for transmissions over IP
- Synchronous and asynchronous transmissions over red and black interfaces
- page 8

High quality of service and flexible operation with state-of-the-art technology

- High quality of service
- Flexible configuration
- Upgradeability
- page 10

Customizable crypto algorithms for specific user requirements

- page 10

Wide selection of accessories simplifies commissioning and operation

- Configuration PC increases the efficiency and accuracy of the preset loading process
- Mounting frame secures the device in physically demanding environments
- R&S®GP3000 data loading device (DLD) enables key distribution to geographically dispersed units
- Seamlessly adjustable external power supply unit (110 V/240 V)
- page 11

DEDICATED OPERATOR INTERFACES FOR VARIOUS APPLICATIONS

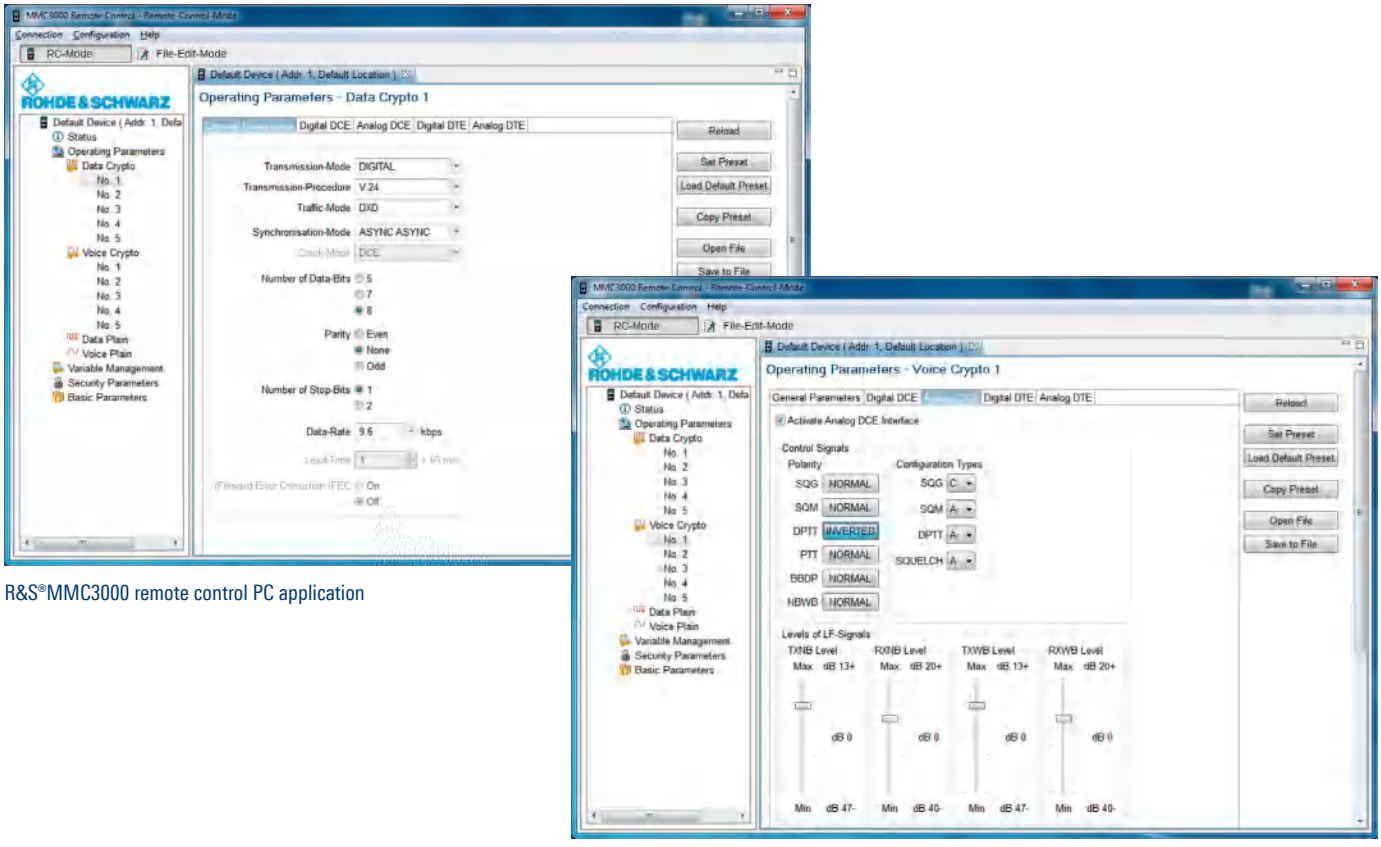
The R&S®MMC3000 offers a wide range of operator interface options supporting different application platforms and scenarios.

Remote control software systems management interface

Full remote control in a defined software environment manages devices in inaccessible locations, e.g. cramped quarters in an aircraft or a naval environment. The application increases flexibility, accuracy and speed in managing a complex system, as up to 31 R&S®MMC3000 can be connected to the RS-485-to-serial adapter. It reduces the probability of error and saves resources by copying repetitive or downloading prepared settings. Presets for a larger number of devices can be stored. This capability is particularly valuable in command and control centers and on board ships – two operating scenarios that typically involve large numbers of detached, external encryption devices and transceivers.

The application also copies and downloads preset parameters (e.g. from one device to another). The five views for each device (status, operating parameters, variable management, security parameters and basic parameters) as well as supervisory activities provide a comprehensive and swift overview of all devices in a group or an overview of all individual device settings at a glance. Existing configuration profiles can now be copied and adapted. This means new devices being readied for installation no longer need to be configured individually – and laboriously – by hand. Configuration can be carried out in a preset management environment. During operation, device configurations can either be left static or, if necessary, can be adapted dynamically.

An interface control document available from Rohde&Schwarz SIT details the interface to the R&S®MMC3000 remote control software, enabling integrators to develop custom remote control software. As a result, the R&S®MMC3000 can be seamlessly integrated into higher-level management systems. In addition, the R&S®MMC3000 remote control software is executable on standard PCs, making its incorporation into existing system environments easy.



R&S®MMC3000 remote control PC application

MIL-bus communications systems management interface

The electronic control of the R&S®MMC3000 MIL-bus interface is accommodated in a separate housing that can be attached to the base unit. It is in line with the MIL-STD-1553B standard including redundant access. The remote control is integrated into an existing communications application and targeted at complex communications systems with a number of R&S®MMC3000 devices – primarily in an airborne environment, e.g. helicopters or fixed-wing aircrafts.

The R&S®MMC3000 MIL-bus module allows full operational capability as well as preset changes and logical zeroize functionality.

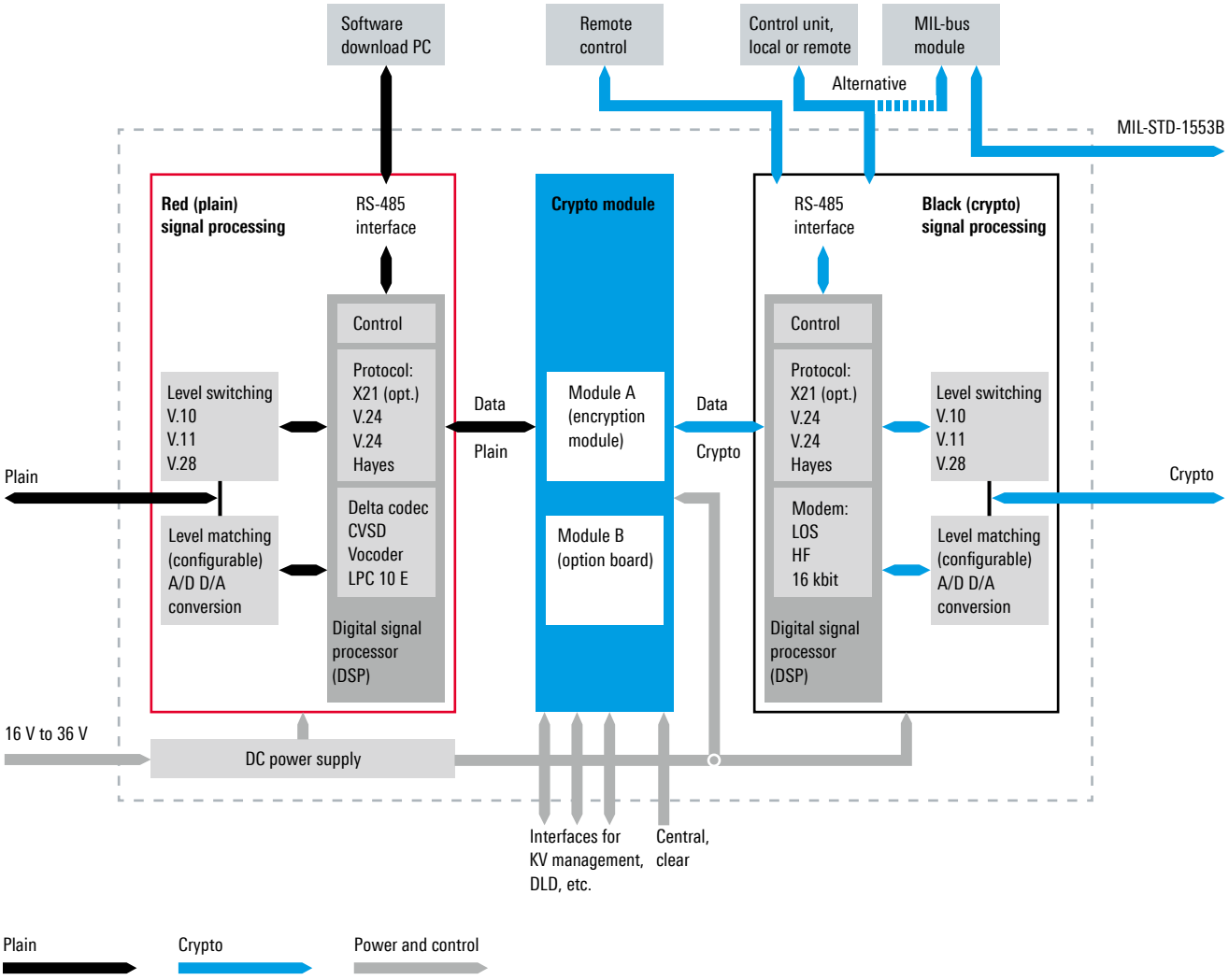
Control unit user interface

The R&S®MMC3000 control unit is accommodated in a separate housing that can be attached to the base unit. It is aimed at simple communications systems with a single R&S®MMC3000, where it enables a local operator to change between presets and to gain access to all logical, physical and security parameter settings (e.g. voltage, physical and logical zeroize, zeroize revocation). Additionally, the control unit can be operated detached from the base unit via a cable link with a cable length of up to 50 m. The connecting parts for the detached control unit are available on request.

Headset/intercom interface

The headset/intercom interface supports both active and passive microphones and squelch for better speech comprehension. It is typically used for local emergency communications or troubleshooting and eliminates the need to reconfigure the connected equipment or applications.

Block diagram of the R&S®MMC3000 crypto device



COMPREHENSIVE PROTECTION THROUGH ELABORATE SECURITY CONCEPT

The R&S®MMC3000 is based on a security concept covering the entire crypto lifecycle to deliver comprehensive protection.

Rear view of the R&S®MMC3000

Audited production environment

The R&S®MMC3000 security concept starts during production, as it is manufactured entirely in a high security environment at audited Rohde&Schwarz plants in Germany.

Hardware red-black separation and tamper protection

Its hardware red-black separation provides the basis for information security on a physical level.

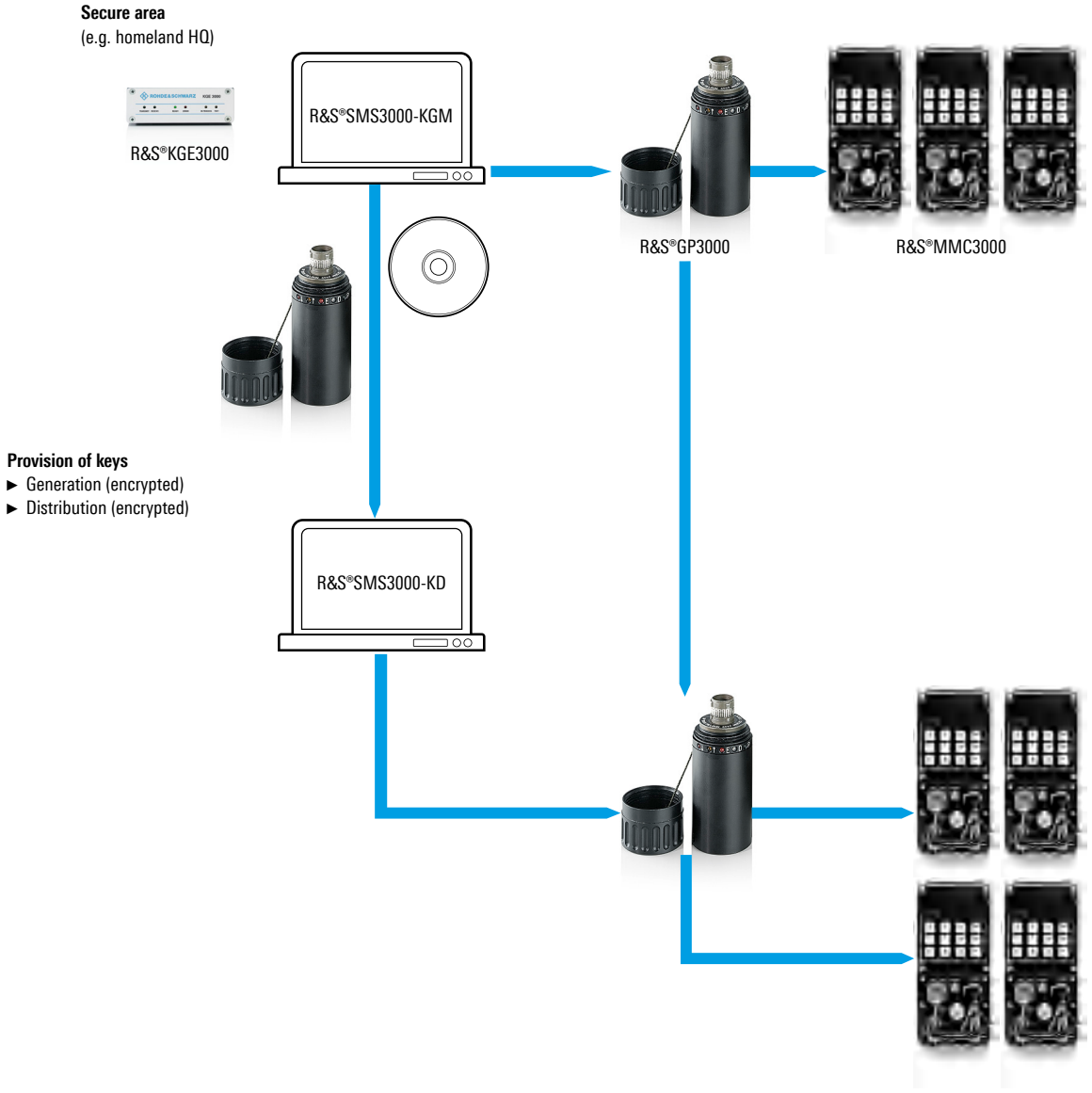
During operation, the integrity of the R&S®MMC3000 is ensured by providing sophisticated tamper protection mechanisms against unauthorized access. In case of emergency, the device can be zeroized automatically or manually at each of the available physical interfaces. Its built-in test equipment (BITE) continuously monitors the device's operation, ensuring correct system behavior. The TEMPEST-proof design eliminates the risk of interception.

Secure key generation and management

The R&S®MMC3000 features modern black crypto variable management as well as a high-performance security management system. Black keys made available by the R&S®SMS3000 security management system are loaded securely from the ruggedized R&S®GP3000 data loading device (DLD) into the R&S®MMC3000. The key generation process is performed on the dedicated R&S®KGE3000 key generation equipment which contains a highest-quality physical true random noise generator (TRNG).

If no key infrastructure is available, the R&S®MMC3000 can generate operational keys at the crypto device.

Key generation and management with the R&S®MMC3000



VERSATILITY THROUGH MULTIPLE TRAFFIC/OPERATING MODES AND TRANSMISSION METHODS

The R&S®MMC3000 flexible interface concept with analog and digital communications interfaces supports a variety of traffic and operating modes and transmission methods.

Traffic modes according to operating modes and transmission methods

The mode the R&S®MMC3000 uses to send voice and data depends on the selected operating mode and transmission method. The available traffic modes are simplex, half duplex (HDX), duplex, double simplex (DX), late entry (DX-LE) and duplex with acknowledgment (DXD).

Operating modes for voice and data transmissions

The R&S®MMC3000 features four operating modes that are determined by the wiring of the external interfaces and by parameterization. The individual operating modes are parameterized via the control unit. The set parameters are stored in the R&S®MMC3000 base unit. The parameterized operating modes are the following:

Data crypto

In data crypto mode, the R&S®MMC3000 can be integrated into data transmission systems equipped with interfaces compatible with ITU-T V.24/V.10/V.11/V.28 or X.21/V.11 (optional). Dialing protocols or Hayes commands (AT commands) can be used. After the Hayes commands sent by the data terminal equipment (STE) have been identified and checked, the R&S®MMC30000 forwards the Hayes commands, synchronizes to the called station and activates the encrypted data mode. If an analog interface is used, the integrated LOS modem (in line with ITU-T V.26) or HF modem (in line with STANAG 4197) is used.

Voice crypto

In voice crypto mode, the voice signals are digitized either by the LPC 10e vocoder or the CVSD delta codec, depending on the traffic mode. An HF modem (in line with STANAG 4197), a LOS modem (in line with ITU-T V.26), baseband/diphase or V.24 mode can be selected, depending on the selected voice digitization method.

Plain voice/plain data

Several plain modes are available for voice and data depending on the different applications (voice: HF, VHF, UHF modes; data; digital V.24 mode).

Various fields of application of the R&S®MMC3000

Teletype for extremely reliable communications

Teletype provides extremely reliable communications in environments with low, varying bandwidth but requires flexible adaptation to low voltage levels.

Baud rates from 50 bit/s up to 64 kbit/s allow communications in a wide range of extreme, specialist scenarios, e.g. low baud rates in helicopter communications, VHF/UHF transmissions.

The headset interface supports both active and passive microphones and squelch for better comprehension. The device can be configured to support guard channel. Local emergency communications are possible over the interface and/or troubleshooting can be carried out without the need to configure connected equipment/applications.

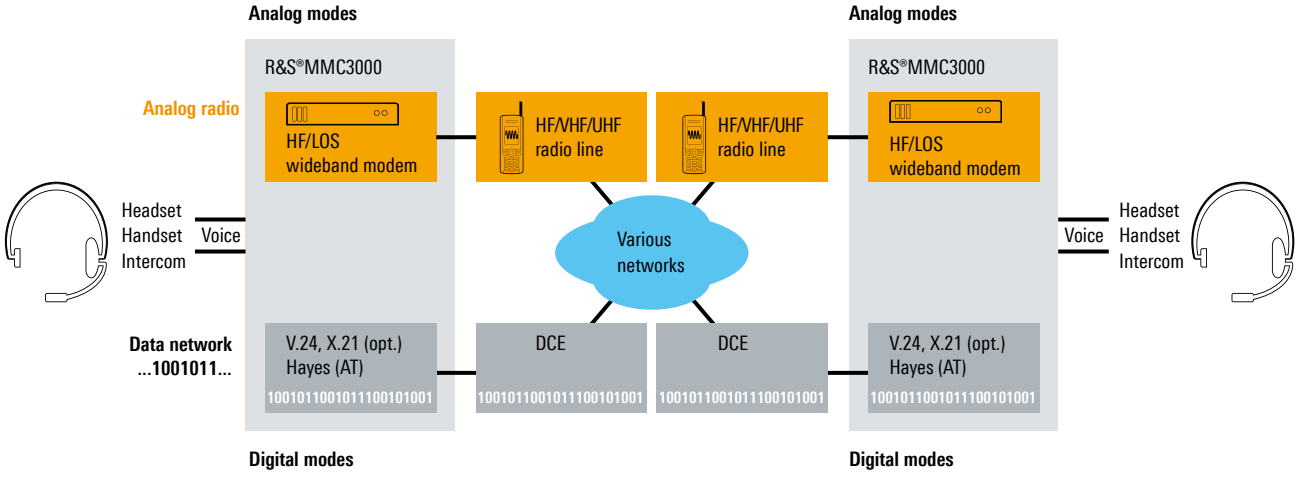
Ready for transmissions over IP

The transition to IP traffic for payload information is supported for Ethernet infrastructures. The data is tunneled through Ethernet using standard converters, removing the distance restrictions for serial transmissions.

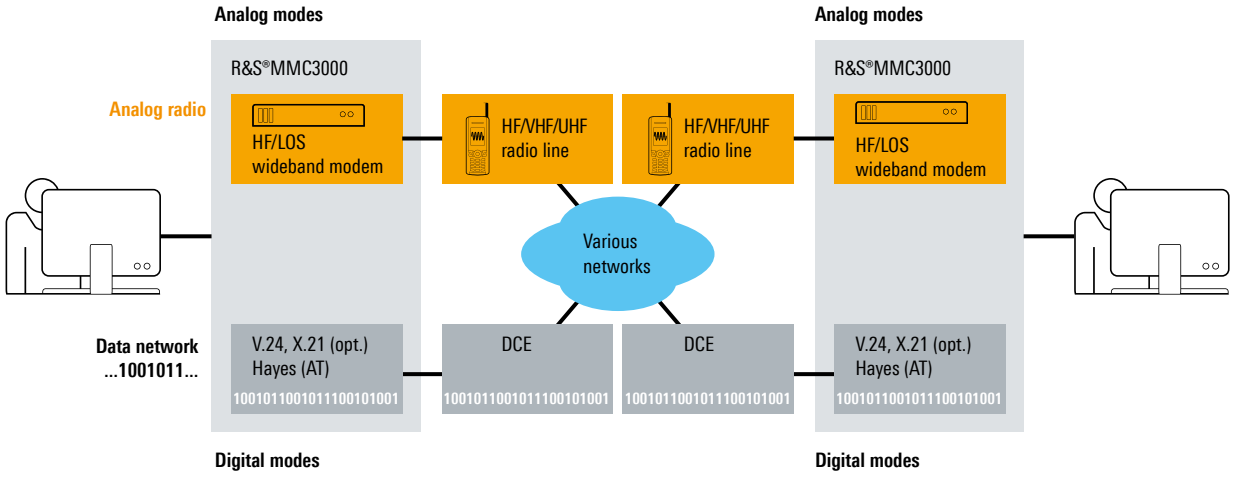
Synchronous and asynchronous transmissions over red and black interfaces

All combinations of synchronous and asynchronous transmissions are supported by both the red and black interfaces. Different clocking requirements within the separate networks are met without the need to introduce additional equipment or modifications to the network.

Voice encryption in various communications networks



Data encryption in various communications networks



HIGH QUALITY OF SERVICE AND FLEXIBLE OPERATION WITH STATE-OF-THE-ART TECHNOLOGY

High quality of service

The R&S®MMC3000 meets the demand for high quality of service under a wide range of conditions:

- Late entry for heavy duty and uninterrupted crypto communications even under demanding transport channel conditions
- High-quality voice codecs optimized for each transmission type

Flexible configuration

Five preset pages for each operating mode provide fast and flexible configuration.

Upgradeability

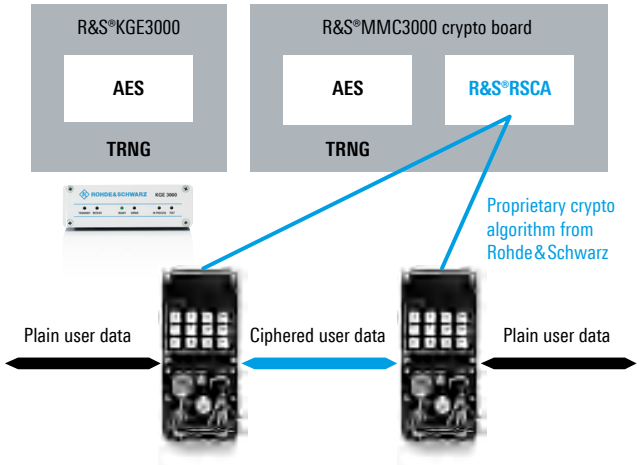
The R&S®MMC3000 provides an extra slot for the integration of a future crypto board.

The R&S®MMC3000 can be upgraded via a protected software download using a PC and a dedicated software download package. This mechanism is secured by the customer-specific crypto algorithm.

CUSTOMIZABLE CRYPTO ALGORITHMS FOR SPECIFIC USER REQUIREMENTS

Encryption in the R&S®MMC3000 is based on the high-performance Rohde&Schwarz SIT crypto board. Specific customer requirements can be accommodated with the proprietary R&S®RSCA algorithm and/or the specific implementation of the AES256 algorithm. The extent of customization can be tailored to suit the exact, unique requirements of various customers and applications. Rohde&Schwarz SIT controls all aspects of the crypto lifecycle so that additional elements, e.g. crypto containers, keying materials, key encryption keys and key loaders, are configured to ensure the seamless and consistent integration of implemented algorithms.

R&S®MMC3000 security technologies



WIDE SELECTION OF ACCESSORIES SIMPLIFIES COMMISSIONING AND OPERATION

Configuration PC increases the efficiency and accuracy of the preset loading process

The application to (pre)configure presets and load them into a number of R&S®MMC3000 devices avoids operator-induced errors when commissioning the device.

Mounting frame secures the device in physically demanding environments

A military-standard mounting frame ensures that the R&S®MMC3000 can be securely fitted in environments particularly prone to jolts, bumps and heavy vibration, e. g. helicopters.

R&S®GP3000 data loading device (DLD) enables key distribution to geographically dispersed units

The DLD eliminates the need to regather all the units to a single location close to the key generation equipment or process. Because it loads black keys into the R&S®MMC3000, the key loading process is secure even if DLDs should be lost.

Seamlessly adjustable external power supply unit (110 V/240 V)

The power supply voltage ranges from 16 V to 36 V. It is EC-protected and features interface options for different plugs.

R&S®MMC3000 components and equipment

USING THE R&S®MMC3000 WITH VARIOUS RADIOS

One of the essential characteristics of modern communications is interoperability with existing equipment. This applies to transceivers as well as crypto units.

Crypto units should also be interoperable with a variety of existing (legacy) and future crypto devices, while playing a variety of roles and supporting diverse modes.

The R&S®MMC3000 was tested with many different radios. It therefore establishes a solid base for interoperable, secure communications with a wide range of vendors.

List of devices tested with the R&S®MMC3000

Manufacturer	Description	Voice mode
BARRETT	890 HF	HF
DICOM	RF13	HF and VHF/UHF
HARRIS	PRC 117F	VHF/UHF
HARRIS	FALCON II RF-5800H	HF and LOS
HARRIS	FALCON II RF-5800U	VHF/UHF
ICOM	IC-M700 Pro	HF
ICOM	IC-706 Pro	HF
Kenwood	TM 241	HF
Kenwood	TS 870	HF
Motorola	URC-200	VHF/UHF
Motorola	MICOM	HF
Raytheon	ARC-232	VHF/UHF
Raytheon	ACU1000	HF and LOS
Rockwell Collins	TALON 8105	VHF/UHF
Rockwell Collins	TALON 8110	VHF/UHF
Rockwell Collins	ARC210	VHF/UHF
Rohde&Schwarz	R&S®M3SR XT4410	VHF/UHF
Rohde&Schwarz	R&S®XK2100	HF
Rohde&Schwarz	R&S®XK4100	HF
Rohde&Schwarz	R&S®XM6923	VHF/UHF
Rohde&Schwarz	R&S®M3AR	VHF/UHF
Rohde&Schwarz	R&S®M3TR	HF and VHF/UHF
Rohde&Schwarz	R&S®XT622P1	VHF/UHF
Rohde&Schwarz	R&S®XT6923L	VHF/UHF
Tait	TB7100	HF and LOS
THALES	TRM6110	HF
THALES	TRM6021	VHF/UHF
THALES	TRG3031C	VHF/UHF
THALES	TRG6031C	VHF/UHF
THALES	TRA6031C	VHF/UHF
THALES	PRC 148	VHF

Note: This list is an indication of the flexibility of the R&S®MMC3000; tests have been performed on individual devices with specific firmware versions and specific applications. For detailed information, please contact Rohde&Schwarz SIT.

SPECIFICATIONS

Specifications		
Operational data		
Operating modes		voice PLAIN/CRYPTO, data PLAIN/CRYPTO
Traffic modes		half duplex (voice), simplex, half duplex (HDX), double simplex (DX), duplex with acknowledgment (DXD), late entry (DX-LE)
Analog interface		
Audio		
Universal four-wire audio/intercom interface		
Level		–47 dB to +13 dB, adjustable in 1 dB steps
Impedance		600 Ω
Headset		headset interface
Radio		narrowband/wideband
Level		–40 dB to +20 dB, adjustable in 1 dB steps
Impedance		600 Ω
Traffic mode		half duplex
Transmission method		BASEBAND/DIPHASE, LOS modem (V.26), HF modem (STANAG 4197)
Voice processing		delta codec (CVSD) 16 kbit/s, LPC 10E (2.4 kbit/s) in line with STANAG 4198
Digital interface		
V.24		asynchronous 50 bit/s to 57.6 kbit/s (5/7/8 bit), async/sync 50 bit/s to 19.2 kbit/s (5/7/8 bit), synchronous 50 bit/s to 64 kbit/s, suitable for Hayes commands
Other interfaces		
Key input		RS-485 (DLD)
Key emergency clearing (zeroize)		switch, central clear
MIL-bus		MIL-STD-1553B
Remote control via PC application	for up to 31 R&S®MMC3000	RS-485
Operating and storage parameters		
Operating temperature range		–30 °C to +70 °C
Storage temperature range		–40 °C to +85 °C
RF leakage		tested
EMC		MIL-STD-461C category A1b, part 2
General data		
Dimensions	W × H × D	90.4 mm × 193.5 mm × 200 mm (3.56 in × 7.62 in × 7.87 in)
Weight		3.8 kg (8.4 lb)
Supply voltage		28 V (16 V to 36 V) DC
Power supply	input	100 V to 240 V AC, 50 Hz to 60 Hz
	output	24 V DC
Power consumption		< 15 VA
MTBF		> 8000 h

ORDERING INFORMATION

Designation	Type	Order No.
Base unit (including base unit, control unit, mounting frame, compact user guide)		
Multimode Multirole Crypto Device	R&S®MMC3000	3566.2805.02
R&S®MMC3000 Manual	R&S®MMC3000	3566.1344.32
R&S®MMC3000 Integrator Manual	R&S®MMC3000	3566.2811.32
R&S®MMC3000 Remote Control Manual	R&S®MMC3000	5401.1635.32
Accessories		
MIL-Bus Module	R&S®MMC3000	3545.0603.03
Control Unit	R&S®MMC3000	3545.0003.03
Mounting Frame	R&S®MMC3000	3544.5330.04
AC Power Supply	R&S®MMC3000	3566.0290.00
Detached Control Unit	R&S®MMC3000	3566.2811.02
Remote Control Software	R&S®MMC3000-RC	5401.1635.00
Fillgun (incl. adapter cable)	R&S®GP3000	3566.2792.02
Key Management Station (incl. R&S®KGE3000)	R&S®SMS3000-KGM	3566.2705.02

YOU ACT. WE PROTECT.

ROHDE&SCHWARZ SIT

Encryption and IT security

Industry

An organization's product ideas, manufacturing processes, patents and financial data make up around 70 percent of its intangible assets. These trade and business secrets are fundamental to the organization's ability to create added value and require special protection. The IT security solutions from Rohde&Schwarz SIT protect companies worldwide against espionage and manipulation of data. The products combine maximum protection with a minimum of administrative effort and offer users an optimum price/performance ratio. The Rohde&Schwarz SIT product portfolio comprises encryption solutions for protecting data transmission in public and private networks, next-generation firewalls for ensuring the secure use of clouds and the Internet, and flexible solutions for tap-proof voice calls.

Critical infrastructures

Critical infrastructures keep our society and economy functioning smoothly. Attempts to manipulate the infrastructures on which energy suppliers, transport operators, emergency services and the financial sector rely could pose a serious threat to public safety. Rohde&Schwarz SIT offers operators of critical infrastructures smart IT security products to secure the control and communications networks between power plants, switch towers, tollbooths, radio masts and network nodes. In addition to encryption solutions for networks and end-to-end communications, hardware security modules (HSM) in public key infrastructures protect corporate campuses and installations from unauthorized access.

Government

A country's internal political dealings encompass a wide range of sensitive topics, including economic and fiscal affairs and energy policy. Internal communications among policymakers, government authorities as well as public safety and security (PSS) agencies need to remain confidential. For more than 20 years, Rohde&Schwarz SIT has been supplying highly secure solutions that ensure absolute confidentiality at all security classification levels. To safeguard their sovereignty, countries can use their own national cryptographic algorithms. The Rohde&Schwarz SIT product portfolio includes encryption products for all classification levels to protect networks and end-to-end communications. The products for government use are approved by Germany's Federal Office for Information Security (BSI) and by the EU and NATO (up to top secret and cosmic top secret security classification levels).

Armed forces

Operations launched to protect societies involve serious risk. Precise, timely information is necessary for strategic command of operations such as peacekeeping, humanitarian aid and disaster relief. Maintaining information superiority has the utmost priority. Rohde&Schwarz SIT, an IT security partner to the Federal Republic of Germany since 2004, is involved in various NATO equipment programs. The company provides solutions for effectively protecting voice, data, images and video transmitted over fixed-networks, radio relay and satellite links. Rohde&Schwarz SIT stands for long-term product availability and the interoperability of solutions with existing equipment. The products for military use are approved by Germany's Federal Office for Information Security (BSI) and by NATO and the EU (up to top secret and cosmic top secret security classification levels).

Service that adds value

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

Rohde&Schwarz

The Rohde&Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

Rohde&Schwarz training

www.training.rohde-schwarz.com

Rohde&Schwarz customer support

www.rohde-schwarz.com/support

PD 0758.2548.12 | Version 05.00 | October 2020 (ch)
R&S®MMC3000 Multimode Multirole Crypto Device
Data without tolerance limits is not binding | Subject to change

0758254812
0758.2548.12 05.00 PDP 1 en