

R&S®CMA180

Radio Test Set

Instrument Security Procedures



1209.7041.02 – 01

1 Overview

In many cases, it is imperative that you use the R&S®CMA180 Radio Test Set in a secured environment. Generally these highly secured environments do not allow any test equipment to leave the area unless it can be proven that no user information leaves with the test equipment. Security concerns can arise when devices need to leave a secured area e.g. to be calibrated or serviced.

This document describes the types of memory and their usage in the R&S®CMA180. It provides a statement regarding the volatility of all memory types and specifies the steps required to declassify an instrument through memory clearing or sanitization procedures. These sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS).

2 Instrument Models Covered

Product	Order number
R&S®CMA180	1173.2000K18

3 Security Terms and Definitions

Clearing

The term "clearing" is defined in Section 8-301a of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)". Clearing is the process of eradicating the data on media so that the data can no longer be retrieved using the standard interfaces on the instrument. Therefore, clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.

Sanitization

The term "sanitization" is defined in Section 8-301b of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)". Sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned for service of calibration.

The memory sanitization procedures described in this document are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are specified in the "Clearing and Sanitization Matrix" in Section 14.1.16 of the ISFO "Manual for the Certification and Accreditation of Classified Systems under the NISPOM".

Instrument declassification

The term "instrument declassification" refers to procedures that must be undertaken before an instrument can be removed from a secure environment, for example when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. The declassification procedures described in this document are designed to meet the requirements specified in DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", Chapter 8.

4 Types of Memory and Information Storage in the R&S®CMA180

This section contains information on the memory components available in the R&S®CMA180.

The following table provides an overview. For more details, refer to the subsequent sections.

Memory type	Size	Content	Volatility	User data	Sanitization procedure
SDRAM	Max. 8 Gbyte	Temporary information storage for CPU, operating system, firmware, waveforms	Volatile	Yes	Shut down the instrument
Flash	Max. 8 Mbyte	Firmware, calibration data, BIOS	Non-volatile	No	None required (no user data)
EEPROM	Max. 2 Mbyte	HW info, serial number, options, calibration data	Non-volatile	No	None required (no user data)
HDD/SSD	Max. 512 Gbyte	Operating system, firmware, instrument data, measurement results, user settings	Non-volatile	Yes	Remove HDD/SSD

4.1 Volatile Memory

The volatile memory in the instrument loses its contents as soon as the instrument is shut down (standby state). The volatile memory does not have battery backup, even if the instrument is equipped with a battery compartment. You do not need to disconnect the power supply, switch off the main power switch on the rear panel or remove batteries.

The volatile memory is not a security concern.

Bringing the instrument to standby state meets the memory sanitization requirements specified in the "Clearing and Sanitization Matrix" in Section 5.2.5.5.5 of the ISFO "Manual for the Certification and Accreditation of Classified Systems under the NISPOM".

SDRAM

The SDRAM on the CPU board and on other boards like R&S CMA-H100 or R&S CMA-H110 has a size of up to 8 Gbyte.

Sanitization procedure: Shut down the instrument

4.2 Non-Volatile Memory

The instrument contains several types of non-volatile memory.

Flash/EEPROM

Each board assembly in the R&S®CMA180 has at least one serial EEPROM device/flash memory with a size of up to 1 Mbyte each. These components contain information related to the installed hardware, for example the board serial number, options and calibration data.

The CPU board of the R&S®CMA180 has 1 Mbyte flash memory which contains the BIOS.

The EEPROM/flash memory does not hold user data nor can the user access the components.

Sanitization procedure: None required (no user data)

Hard disk drive (HDD)/solid state disk (SSD)

The R&S®CMA180 is equipped with a removable system drive (HDD or SSD) with a size of up to 512 Gbyte.

It contains miscellaneous information, for example:

- Operating system (Windows 7 embedded®, 64 bit)
- Firmware, instrument states and setups
- Log files
- Measurement results
- Screen images
- Other files stored by the user in the Windows file system

Sanitization procedure: Remove the HDD/SSD from the instrument

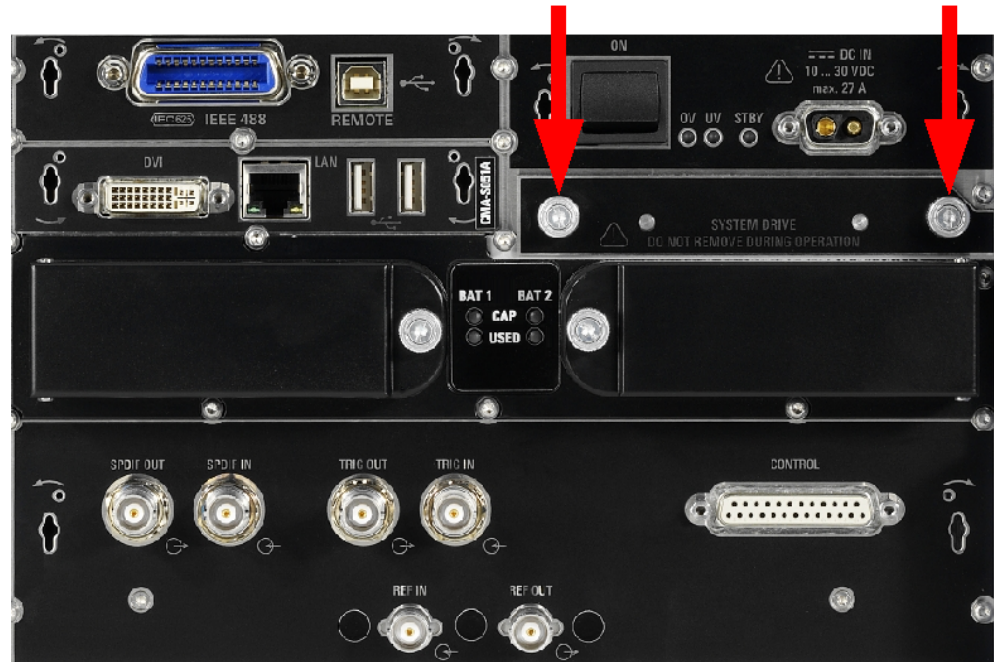
5 Instrument Declassification

User data can be contained in the SDRAM and on the system drive (HDD or SSD). Before you move the instrument out of a secured area, erase the SDRAM and remove the system drive as described in this section. Do not open the instrument.

Initial situation: The instrument is supplied with power and running.

Proceed as follows:

1. Press the standby key in the lower left corner of the front panel.
Wait until the LEDs above the key have changed from green to yellow.
This action shuts down the instrument, erases the SDRAM and is a prerequisite for removing the system drive.
2. On the rear panel, unscrew the two knurled screws.



3. Remove the system drive.

You have now removed all user data from the R&S®CMA180. The R&S®CMA180 can leave the secured area.

Once the R&S®CMA180 is outside of the secured area, equip it with a non-classified system drive without any user data. Thus, the R&S®CMA180 works properly for service or other needs.

Prior to re-entering the secured area, remove the non-classified system drive (without the user data). When the R&S®CMA180 is back in the secured area, you can put the original classified system drive back into the instrument.



To store classified user data, use the system drive that is delivered with the R&S®CMA180.

Validity of the calibration after removing the system drive

The EEPROM/flash memory is the only memory type used to hold calibration data. Therefore, removing or exchanging the system drive does not affect the validity of the calibration.

6 Special Considerations for USB Ports

USB ports can pose a security threat in high-security locations. Generally, this threat comes from small USB pen drives, also known as memory sticks or key drives. They can be easily concealed and can quickly read/write several Gbyte of data.

Disabling USB ports for writing user data

You can disable the write capability on the USB ports of the R&S®CMA180 via a utility software. This utility software is available on the CMA customer web.

The CMA customer web is a section of GLORIS, the "Global Rohde & Schwarz Information System", see <https://extranet.rohde-schwarz.com>. A registration is required.

To disable the write capability, copy the utility software to the R&S®CMA180 and run it once. After a reboot of the instrument, the write capability on any USB memory device is disabled.

© 2016 Rohde & Schwarz GmbH & Co. KG

Mühlhofstr. 15, 81671 München, Germany

Phone: +49 89 41 29 - 0

Fax: +49 89 41 29 12 164

Email: info@rohde-schwarz.com

Internet: www.rohde-schwarz.com

Subject to change – Data without tolerance limits is not binding.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.

Trade names are trademarks of the owners.