R&S®SGS100A
SGMA RF Source
Instrument Security Procedures

ROHDE&SCHWARZ

Instrument Security Procedures

Version 05

Contents

1 Overview

It is often imperative that R&S SGS SGMA RF Sources are used 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 SGS. 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

Table 2-1: SGMA RF Source models

Product name	Order number
R&S SGS100A	1416.0505.02

The SGMA RF Source base unit must be ordered together with one of the following frequency options:

- R&S SGS-B106
- R&S SGS-B106V

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 SGS

The R&S SGS contains various memory components.

The following table provides an overview of the memory components that are part of your instrument. For a detailed description regarding type, size, usage and location, refer to the subsequent sections.

Memory type	Size	Content	Volatility	User data	Sanitization procedure
SDRAM (Controller board)	2 Gbit	Temporary information storage for operating system and instrument firmware	Volatile	Yes	Turn off instrument power
EEPROM (one per module)	4 x 4 kbyte up to 1 Mbyte	Module-specific data: • Board identification data • Board internal correction data	Non-volatile	No	None required (no user data)
Smart card / SIM (Controller board)	68 kbyte	Module-specific data: • Device ID • Product options • Operation time • Power-on count	Non-volatile	No	None required (no user data)
Flash (Controller board)	2 Gbit	• Operating system • Instrument firmware • Boot code • Maintenance and recovery system • User data, instrument and password settings	Non-volatile	Yes	Sanitize internal memory

4.1 Volatile Memory

The volatile memory in the instrument does not have battery backup. It loses its contents when power is removed from the instrument. The volatile memory is not a security concern.

Removing power from this memory 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".

4.2 Non-Volatile Memory

The R&S SGS contains various non-volatile memories. Out of these memories, only the internal Flash memory contains user data and instrument configuration in its Journaling Flash File System (JFFS) section.

Basically, the R&S SGS provides a sanitizing procedure (see Sanitize internal memory) that removes user data irretrievably from the instrument. In addition, you can activate the volatile mode on the R&S SGS. When enabled, this mode protects the Flash memory from writing, and redirects the user data to the volatile SDRAM.

All non-volatile memories of the R&S SGS are not a security concern.

Flash (controller board)

The single-chip Flash memory consists of three logical sections.

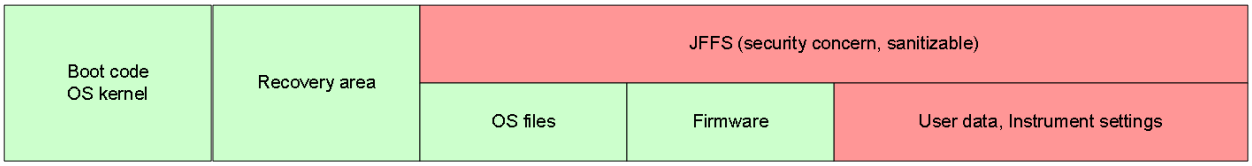

Figure 4-1: Logical sections of the Flash memory

- **Boot code/OS kernel:**
  The 8 Mbyte memory section contains the boot code and the operating system kernel. This section is initialized during production and can be updated in case of firmware update. It cannot be accessed and is not modified during instrument operation.
- **Recovery area:**
  The 64 Mbyte memory section contains recovery data which is used to restore the factory instrument configuration if necessary. This section is initialized with the instrument first setup. It cannot be accessed and is not modified during instrument operation.
- **Journaling flash file system (JFFS):**
  The remaining memory section is controlled by the JFFS. This area is shared between operating system files, instrument firmware and user data. Operating system files and instrument firmware are encapsulated in preconfigured, read-only squash FS file systems. Both cannot be modified during instrument operation nor can they be modified in parts. During firmware update, they are replaced in total.

  The remaining JFFS section contains the following information:

  – User data and instrument settings (automatically or manually saved instrument setups)
  – Passwords
  – LAN and USB port enable/disable states
  – Internal adjustment data

The R&S SGS provides a sanitizing procedure that ensures that user data is irretrievably removed from the instrument.

The sanitization procedure for the JFFS section, which holds user data depends on the setting of the volatile mode.

- If the volatile mode is disabled (default setting on the instrument):
  The R&S SGS saves user data and instrument setups permanently on the Flash memory.
  Sanitization procedure: Sanitize internal memory
- If the volatile mode is enabled:
  The Flash memory is write protected. The R&S SGS redirects user data and instrument setups to the volatile memory SDRAM.
  Sanitization procedure: Turn off instrument power

5 Secure Erase Procedures

The sanitizing procedure is part of the instruments maintenance system.

Sanitize internal memory

To start the sanitizing procedure:

► During power-on, press the front panel buttons [RF], [LAN] and [ID].

When started, the sanitizing procedure executes the following steps:

- The file `rootfs.squashfs` (read-only, encapsulating operating system files) and the file `optfs` (read-only, encapsulating instrument firmware) are temporarily saved in the SDRAM.
- A full sector erase command is applied to each sector of the JFFS partition. This command explicitly includes sectors which might be declared as defect.
- Each addressable location of the JFFS section is overwritten by a single character.
- A second full sector erase command is applied to each sector of the JFFS area, including defect sectors.
- The JFFS is recreated and the operating system files and instrument firmware are restored.
- Passwords are reset to factory values, USB and Ethernet interfaces are enabled.

The Secure Erase Procedures meet the memory sanitization requirements 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".

6 Instrument Declassification

Before you can remove the R&S SGS from a secured area (for example to perform service or calibration), all classified user data needs to be removed. You can declassify the instrument as follows:

1. To sanitize the volatile memory, turn off the R&S SGS.
2. To sanitize the non-volatile memory (Flash memory), perform the following steps:
   a) Make sure, that you have not connected a USB mass memory device.
   b) Press the front panel buttons [RF], [LAN] and [ID] and hold them while turning on the instrument again.

   After a few seconds, the maintenance system is indicated by flashing LEDs.

   Sanitizing starts. Erasing the non-volatile memory is indicated on the front panel by a progress bar of red or orange LEDs while the first LED of the progress bar is flashing.

   When flashing stops, the result is indicated by the LEDs:
   - All LEDs are green: Sanitizing was successful

- All LEDs are red (with one flashing orange): Sanitizing failed
  In this case, retry sanitizing or contact the Rohde & Schwarz service department.

Afterwards the power can be removed or the instrument can be rebooted. During the first reboot after sanitizing the R&S SGS executes internal adjustments. Since permanent adjustment values are located in the instrument's EEPROMs, the validity of the instrument's calibration is maintained throughout the sanitization.

Following these steps removes all user data from the R&S SGS. The instrument can now leave the secured area.

These declassification procedures meet the needs of customers working in secured areas.

Validity of instrument calibration after declassification

The calibration makes sure that measurements comply to government standards. Rohde & Schwarz recommends that you follow the calibration cycle suggested for your instrument.

The EEPROM is the only memory type used to hold permanent adjustment values required to maintain the validity of the R&S SGS's calibration. Therefore, performing the declassification procedure does not affect the validity of the instrument's calibration.

7 Special Considerations for USB Ports and LAN Services

There are special considerations for R&S SGS USB ports and LAN services to avoid unauthorized data access in a high-security location.

7.1 Special Considerations for USB Ports

USB ports can pose a security risk in high-security locations. Generally, this risk 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

Remove all USB memory devices before disabling the USB storage. If any USB memory device remains connected, disabling is blocked, and the instrument returns a warning message.

You can disable the USB ports of the R&S SGS in the "SGS: Security" dialog:

1. In the "SGMA GUI", select "Instrument Name" > "Setup" > "Security".
2. In the "Security Settings" section, select "USB Device" > "Disable".
3. Enter the "Security Password" and confirm with "Accept".

   When disabled, the R&S SGS does not accept any USB memory device. Other non-memory USB devices (such as keyboards and mice) are not affected.

The R&S SGS saves the state of the USB port on the Flash memory, see "Flash (controller board)" on page 4.

7.2 Special Considerations for LAN Ports

To protect the instrument against unauthorized data access in your high-security location, you can disable the LAN interface.

Disabling LAN ports

You can disable the LAN ports of the R&S SGS in the "SGS: Security" dialog:

1. In the "SGMA GUI", select "Instrument Name" > "Setup" > "Security".
2. In the "Security Settings" section, select "LAN Connectors" > "Disable".
3. Enter the "Security Password" and confirm with "Accept".

   When disabled, you cannot establish a LAN connection to the instrument.

The R&S SGS saves the state of the LAN port on the Flash memory, see "Flash (controller board)" on page 4.

For more information concerning the security features, refer to the user manual of the R&S SGS, see www.rohde-schwarz.com/manual/sgs100a.

Mühldorfstr. 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