R&S®SGU100A
SGMA Upconverter
Instrument Security Procedures

1176.9729.02 ─ 02

ROHDE&SCHWARZ

Contents

1 Overview

In many cases, it is imperative that the R&S SGU SGMA Upconverters 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 SGU. 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 Upconverter models

Product name	Order number
R&S SGU100A	1416.0808.02

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

- R&S SGU-B120
- R&S SGU-B120V

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 SGU

The SGMA Upconverter 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 (CPU board)	256 Mbyte	Temporary information storage for operating system and instrument firmware	Volatile	Yes	Turn off instrument power
EEPROM (RF module, processor module)	4 x 4 kbyte up to 1 Mbyte	• Module-specific data: – Serial number – Revision – Options • Calibration correction data • Initial CPU configuration data	Non-volatile	No	None required (no user data)
Smart card (processor module)	32 kbyte	Hardware information: • Serial number • Product options • Operation time • Power-on count	Non-volatile	No	None required (no user data)
Flash (processor board)	256 Mbyte	• Operating System • Instrument firmware • Boot code • Maintenance and recovery system • User data, instrument and password settings	Non-volatile	Yes	"Sanitize internal memory" procedure (see "Flash" on page 5)

4.1 Volatile Memory

The volatile memory in the instrument does not have battery backup. It loses its contents as soon as 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 Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.

SDRAM

The SDRAM on the CPU board has a size of 256 Mbyte and contains temporary information storage for operating system and instrument firmware. The SDRAM loses its memory as soon as power is removed.

Sanitization procedure: Turn off instrument power

4.2 Non-Volatile Memory

The R&S SGU contains various non-volatile memories. Out of these, only the internal Flash memory contains user data as well as instrument configuration in its Journaling

Flash File System (JFFS) area. The Flash memory can be sanitized via "Sanitize internal memory" procedure.

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

EEPROM

The RF module as well as the processor module of the R&S SGU SGMA Upconverter are equipped with in total four serial EEPROM devices with a size of 4 kbyte up to 1 Mbyte. The EEPROMs contain module-specific data, calibration correction data and initial processor configuration data. The EEPROM does not hold user data nor can the user access the EEPROM storage.

Sanitization procedure: None required (no user data)

Smart card

The processor module of the R&S SGU SGMA Upconverter is equipped with a smart card with a size of 32 kbyte. It contains information related to the installed hardware, such as the serial number of the module, product options, operating time and power-on cycle count. The smart card does not hold user data nor can the user access the storage.

Sanitization procedure: None required (no user data)

Flash

The single-chip Flash memory, located on the processor board, has a size of 256 Gbyte of storage. The Flash contains boot code, maintenance and recovery system, the operating system and instrument firmware. Furthermore user data, instrument and password settings are stored here.

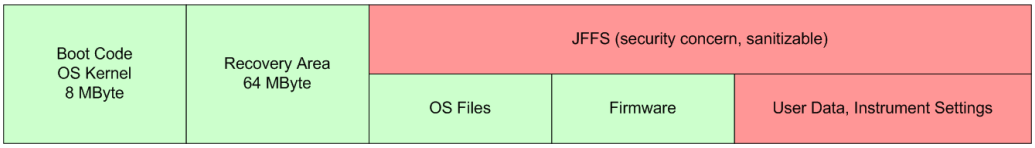

Figure 4-1: Logical sections of the Flash memory

The Flash memory is logically divided into three sections:

- **Boot code/OS kernel:**
  The 8 Mbyte memory section contains the boot code and the operating system kernel. This area is initialized during production and can be updated in case of firmware update. It cannot be accessed by the user 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 required. This area is initialized during production. It cannot be accessed by the user and is not modified during instrument operation.

- **Journaling Flash File System (JFFS):**
  The remaining memory section is controlled by a Journaling Flash File System (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.

  In the remaining JFFS area the following information is stored:

  – 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 SGU provides a sanitizing procedure that ensures that user data is irretrievably removed from the instrument.

Sanitization procedure: "Sanitize internal memory" procedure

The sanitizing procedure is part of the instruments maintenance system which can be accessed by pressing the front panel buttons RF, LAN and ID during power-on.

After activating the sanitizing procedure, the following steps occur:

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

The "Sanitize internal memory" procedure meets 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".

5 Instrument Declassification

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

1. Turn off the SGMA Upconverter. This will sanitize the volatile memory.

2. To sanitize the internal Flash memory, perform the following steps:

   a) Make sure, that no USB mass memory device is connected.
   b) Press the front panel buttons RF, LAN and ID and hold them while switching on the instrument again.

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

   Sanitizing starts now. Erasing the Flash memory is indicated by a running red LED.

   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 internal adjustments are performed. Since permanent adjustment values are located in the instrument's EEPROMs, the validity of the SGMA Upconverter's calibration is maintained throughout the sanitization.

Following these steps removes all user data from the SGMA Upconverter. The SGMA Upconverter 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 SGU's calibration. Therefore, performing the declassification procedure does not affect the validity of the instrument's calibration.

6 Special Considerations for USB Ports and LAN Services

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

6.1 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

You can disable the USB ports of the R&S SGU in the setup dialog:

1. Select "Setup", "Security", "USB Storage" and then "Disable".
2. Enter the **Security Password** and confirm with "Accept".

   When disabled, no USB storage device is accepted by the instrument. Other non-memory USB devices (such as keyboards and mice) are not affected.

The enable/disable state of the USB port is stored on the Flash memory.

6.2 Special Considerations for LAN Ports

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

Disabling LAN ports

You can disable the LAN ports of the R&S SGU in the setup dialog:

1. Select "Setup", "Security", "LAN Services" and disable "LAN Interface".
2. Enter the **Security Password** and confirm with "Accept".

   When disabled, no LAN connection can be established with the instrument.

The enable/disable state of the LAN port is stored on the Flash memory.

For more information concerning the security features, refer to the R&S SGU100A Operating Manual.

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

Throughout this manual, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®SGU is indicated as R&S SGU.