R&S®FPC
Spectrum Analyzer
Instrument Security Procedures

1178644002
Version 02

ROHDE&SCHWARZ
Make ideas real

Contents

1 Overview....2
2 Instrument Models Covered....3
3 Security terms and definitions....3
4 Types of Memory and Information Storage....4
5 Instrument Declassification....7

1 Overview

Securing important information is crucial in many applications.

Generally, 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, e.g. to be calibrated.

"Regarding sanitization, the principal concern is ensuring that data is not unintentionally released" [1].

This document provides a statement regarding the volatility of the memory types used and specifies the steps required to sanitize an instrument.

The procedures in this document follow "NIST Special Publication 800-88: Guidelines for Media Sanitization" [1].

In addition, recommendations are provided to safeguard information on the R&S FPC.

References

See the following literature for further information.

[1] **Kissel Richard L. [et al.]** Guidelines for Media Sanitization = Special Publication (NIST SP) = NIST SP - 800-88 Rev 1. - Gaithersburg : [s.n.], December 17, 2014.

[2] **National Industrial Security Program Authorization Office** Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM). - May 6, 2019.

[3] **ACSC Australian Cyber Security Centre** Australian Government Information Security Manual, January 2020.

2 Instrument Models Covered

Table 2-1: Spectrum Analyzer models

Product name	Order number
R&S FPC1000	1328.6660.02
R&S FPC1500	1328.6660.03

3 Security terms and definitions

Terms defined in Guidelines for Media Sanitization

NIST Special Publication 800-88 [1]

- **Sanitization**
  "Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort."
- **Clear**
  "Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported)."
- **Purge**
  "Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques."
- **Destroy**
  "Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data."

Control of media

Another option to secure sensitive information is to keep physical media within the classified area, see [1], paragraph 4.4.

Volatile memory

"Memory components that do not retain data after removal of all electrical power sources, and when reinserted into a similarly configured system, are considered volatile memory components." [2]

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

If the instrument is battery operated, e.g. handhelds, it retains data in the volatile memory as long as the battery is installed.

Typical examples are RAM, e.g. SDRAM.

Non-volatile memory

"Components that retain data when all power sources are discontinued are non-volatile memory components." [2].

In the context of this document, non-volatile memory components are non-user accessible internal memory types, e.g. EEPROM, Flash, etc.

Media

Media are types of non-volatile memory components. In the context of this document, media are user-accessible and retain data when you turn off power.

Media types are Hard Disk Drives (HDD), Solid State Drives (SSD), Memory Cards, e.g. SD, microSD, CFast, etc., USB removable media, e.g. Pen Drives, Memory Sticks, Thumb Drives, etc. and similar technologies.

4 Types of Memory and Information Storage

The R&S FPC Spectrum Analyzer 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	512 Mbyte	Temporary information storage for operating system and instrument firmware	Volatile	Yes	Turn off instrument power
Flash (µC internal)	32 kbyte	Power-up / Power-down firmware	Non-volatile	No	None required
SRAM (µC internal)	4 kbyte	Temporary information storage for Power-up / Power-down firmware	Volatile	No	Turn off instrument power
Flash	128 Mbyte	• Operating System • Instrument firmware • Boot code • Calibration correction data, product options and serial number • User data and instrument 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 512 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.

SRAM (µC)

The SRAM of the µController has a size of 4 kbyte and contains temporary information storage for Power-up / Power-down firmware. The SRAM loses its memory as soon as power is removed.

Sanitization procedure: Turn off instrument power

4.2 Non-Volatile Memory

The R&S FPC contains various non-volatile memories. Out of these, only the internal Flash memory contains user data as well as instrument configuration. The Flash memory can be sanitized via "Sanitize internal memory" procedure.

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

Flash (µC)

The µController internal flash memory has a size of 32 kbyte and contains the µController firmware for the Power-up / Power-down sequence. The flash does not hold user data nor can the user access the flash storage.

Sanitization procedure: None required (no user data)

Flash

The flash memory has a size of 128 Mbyte of storage. It contains the boot code, operating system and instrument firmware, calibration correction data of product options and serial number. Furthermore user data and instrument settings are stored here.

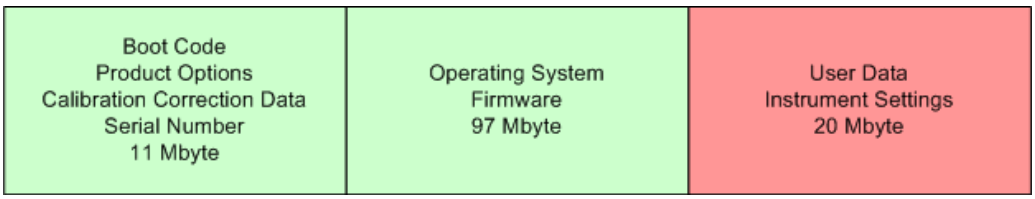

Figure 4-1: Logical sections of the Flash memory

The Flash memory is logically divided into three sections:

- **Boot Code / Product Options / Calibration Correction Data / Serial Number:**
  The 11 Mbyte memory section contains the boot code, the product options, the factory calibration correction data and the instrument serial number. This section is initialized during production and can be updated in case of firmware update and option installation. It cannot be accessed by the user and is not modified during instrument operation.
- **Operating System / Firmware:**
  The 97 Mbyte memory section contains the operating system and the instrument firmware. This section 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.
- **User Data / Instrument Settings:**
  The 20 Mbyte memory section contains the user data and automatically or manually saved instrument settings.

The R&S FPC 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 [PRESET] and softkey [5] during power-on.

After activating the sanitizing procedure, the following steps occur:

- A full sector erase command as per manufacturer data sheet is applied to each sector of the instrument settings and user data section. This explicitly includes sectors which might be declared as defect.
- Every addressable location of the instrument settings and user data section is overwritten by a single character.
- Again, a full sector erase command as per manufacturer data sheet is applied to each sector of the instrument settings and user data section, including defect sectors.

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

1. Turn off the R&S FPC. 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 [PRESET] and softkey [5] and hold them while switching on the instrument again.

   After a few seconds, the sanitizing procedure starts.

   Sanitizing is indicated by the message "Secure Formatting Flash, please wait!" on the instrument's screen. The sanitizing procedure takes approximately 8 minutes.

Afterwards, the instrument reboots. Since permanent adjustment values are not located in instrument settings and user data section of the flash, the validity of the R&S FPC Spectrum Analyzer’s calibration is maintained throughout the sanitization.

Following these steps removes all user data from the R&S FPC Spectrum Analyzer. 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 flash is the only memory type used to hold permanent adjustment values required to maintain the validity of the R&S FPC's calibration.

Since only the flash instrument settings and user data section is erased during sanitization, performing the declassification procedure does not affect the validity of the instrument’s calibration.

Muehldorfstr. 15, 81671 Muenchen, Germany
Phone: +49 89 41 29 - 0
Email: info@rohde-schwarz.com
Internet: www.rohde-schwarz.com

Throughout this document, products from Rohde & Schwarz are indicated without the ® symbol and without the model designation, e.g. R&S®FPC1000 is indicated as R&S FPC.