R&S®FPS
Signal and Spectrum Analyzer
Instrument Security Procedures

1176.9093.02 ─ 04

ROHDE&SCHWARZ

Contents

1 Overview

In many cases, it is imperative that the R&S FPS Signal and Spectrum Analyzers 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 FPS. 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 name	Order number
R&S FPS4	1319.2008.04
R&S FPS7	1319.2008.07
R&S FPS13	1319.2008.13
R&S FPS30	1319.2008.30
R&S FPS40	1319.2008.40

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 FPS

The Signal and 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 (CPU board)	16 Gbyte	Temporary information storage for operating system and instrument firmware	Volatile	Yes	Turn off instrument power
SDRAM/DDR3 (detector board)	2 Gbyte	Measurement data	Volatile	Yes	Turn off instrument power
EEPROM (board assembly)	16 Mbyte	Hardware information: • Serial number • Product options • Calibration correction data	Non-volatile	No	None required (no user data)
Flash (CPU board)	8 Mbyte	BIOS	Non-volatile	No	None required (no user data)
Solid-State Drive (SSD) (removable)	Variable	• Operating system • Instrument firmware and firmware options with license keys • Instrument states and setups • Trace data • Limit lines, transducer tables • Screen images	Non-volatile	Yes	Remove SSD from instrument

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 16 Gbyte 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

SDRAM/DDR3

The SDRAM/DDR3 on the detector board has a size of 2 Gbyte and contains measurement data. It loses its memory as soon as power is removed.

Sanitization procedure: Turn off instrument power

4.2 Non-Volatile Memory

The R&S FPS contains various non-volatile memories. Out of these, only the removable Solid-State Drive (SSD) contains user data. The SSD can be physically removed from the R&S FPS and left in the secure area.

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

EEPROM

Each board assembly in the R&S FPS Signal and Spectrum Analyzer has one serial EEPROM device with a size of up to 16 Mbyte. It contains information related to the installed hardware, such as board serial number, product options and calibration correction data. The EEPROM does not hold user data nor can the user access the EEPROM storage.

Sanitization procedure: None required (no user data)

Flash

The CPU board of the R&S FPS Signal and Spectrum Analyzer has one 8 Mbyte of Flash memory. It contains the BIOS. The Flash memory does not hold user data nor can the user access the Flash memory.

Sanitization procedure: None required (no user data)

Solid-State Drive (SSD)

The removable SSD is located on the rear of the R&S FPS. Its size depends on the model you have ordered.

The SSD is used to store:

- Operating system
- Instrument firmware and firmware options (measurement personalities) with option license keys
- Instrument states and setups
- Trace data
- Limit lines, transducer tables
- Screen images

The SSD holds user data and is non-volatile. Hence, user data is not erased when power is removed from the instrument.

The removable SSD can be removed from the Signal and Spectrum Analyzer to make sure that no user data is stored within the Signal and Spectrum Analyzer. This can be done without opening the instrument.

If you are using the optional Secure User Mode, the SSD is write-protected and does not contain permanent user data. In that case, no sanitization procedure is required.

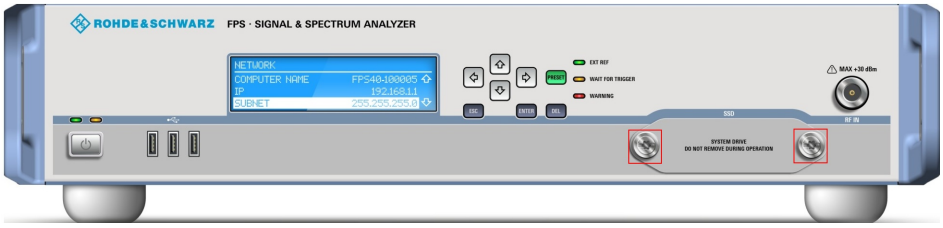
The R&S FPS, equipped with the removable SSD, addresses the needs of customers working in highly sensitive areas.

Sanitization procedure: Remove SSD from instrument

5 Instrument Declassification

Before you can remove the Signal and 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 Signal and Spectrum Analyzer as follows:

1. Turn off the Signal and Spectrum Analyzer. This will sanitize the volatile memory.
2. To remove the classified Solid-State Drive (containing user data), perform the following steps:
   a) Locate the SSD.



   b) Unscrew the two knurled screws.
   c) Remove the Solid-State Drive at the front of the device.

Following these steps removes all user data from the Signal and Spectrum Analyzer. The Signal and Spectrum Analyzer can now leave the secured area.

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

Once the R&S FPS is outside the secured area, installing a second non-classified removable Solid-State Drive (without any user data) allows the R&S FPS to function properly for service or other needs.

Prior to re-entering the secured area, remove the non-classified removable Solid-State Drive (without the user data). When the R&S FPS is back within the secured area, the original classified removable SSD can be reinstalled.

- To hold classified user data in secure areas, use the removable Solid-State Drive which comes with the instrument.
- To hold non-classified user data in non-secure areas, use a second removable Solid-State Drive (R&S FPS-B18).

Secure User Mode

If it is not possible to remove the SSD and store it securely, or if users must not obtain knowledge of other user's data, an optional Secure User Mode (R&S FPS-K33, Security Write Protection) is available. In Secure User Mode, the SSD is write-protected so that no information can be written to memory permanently. Data that the R&S FPS nor-

mally stores on the SSD is redirected to volatile memory instead, which is not a security concern.

Data that is stored in volatile memory can be accessed by the user just as in normal operation. However, when the instrument's power is removed, all data in this memory is cleared. Thus, in Secure User Mode, the instrument always starts in a defined, fixed state when switched on.

Validity of instrument calibration after declassification

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

The R&S FPS stores the adjustment values required to maintain the validity of the calibration on the EEPROM. Therefore, replacing one removable SSD with another does not affect the validity of the instrument calibration.

After exchanging the removable SSD, perform a self-alignment via mini display or remote desktop once:

Note that the instrument has sufficient warm-up time before you perform the self-alignment.

1. Usage of R&S FPS mini display:
   Select "System Commands" and "Selfalign".
2. Usage of a remote desktop connection to the R&S FPS:
   Select "Setup", "Alignment " and "Start Self Alignment".

This function uses the high-stability internal reference generator to produce the temporary adjustment values. Using the permanent and temporary values, the necessary adjustment information is then stored on the removable SSD. Rohde & Schwarz recommends that you perform the self-alignment function once a week.

6 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 for writing user data

You can disable the write capability on the USB ports of the R&S FPS via a utility software. This utility software is available on the R&S FPS website (https://www.rohde-schwarz.com/manual/r-s-fps-instrument-security-manuals-gb1_78701-54618.html).

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

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®FPS is indicated as R&S FPS.