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

1173998602
Version 09

ROHDE&SCHWARZ
Make ideas real

Contents

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 FSW.

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

Product name	Order number
R&S FSW8	1312.8000.08
R&S FSW13	1312.8000.13
R&S FSW26	1312.8000.26
R&S FSW43	1312.8000.43
R&S FSW50	1312.8000.50
R&S FSW67	1312.8000.67
R&S FSW85	1312.8000.85
R&S FSW8	1331.5003.08
R&S FSW13	1331.5003.13
R&S FSW26	1331.5003.26
R&S FSW43	1331.5003.43
R&S FSW50	1331.5003.50
R&S FSW67	1331.5003.67
R&S FSW85	1331.5003.85

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 Statement of volatility

The R&S FSW contains various memory components. See the subsequent sections for a detailed description regarding type, size, usage and location.

Notes on memory sizes

Due to the continuous development of memory components, the listed values of memory sizes may not represent the current, but the minimal configuration.

4.1 Volatile memory

Volatile memory modules are considered as non-accessible internal storage devices, as described in Security terms and definitions > Volatile memory.

Table 4-1: Types of volatile memory

Memory type	Location	Size	Content / Function	User modifiable
SDRAM	CPU board	IPC10: 8 Gbyte IPC11: 16 Gbyte	Temporary information storage for operating system and instrument firmware	Yes
SDRAM/DDR3	Detector board	2 Gbyte	Measurement data	Yes
SDRAM/DDR3	optional B160/B320 bandwidth extension	6 Gbyte	Measurement data	Yes
SDRAM/DDR3	optional B500 bandwidth extension	2 Gbyte	Measurement data	Yes
SDRAM/DDR3	optional B1200/B2001/ B800R bandwidth extension	8 Gbyte	Measurement data	Yes
SDRAM/DDR3	optional B4001/B6001/ B8001 bandwidth extension	24 Gbyte	Measurement data	Yes

4.2 Non-volatile memory

Non-volatile memory modules are considered as non-accessible internal storage devices, as described in Security terms and definitions > Non-volatile memory.

Table 4-2: Types of non-volatile memory

Memory type	Location	Size	Content / Function	User modifiable
EEPROM	Board assembly	1 Mbyte	Hardware information: • Serial number • Product options • Calibration correction data	No
Flash	CPU board	IPC10: 1 Mbyte IPC11: 8 Mbyte	BIOS	No

4.3 Media

Media memory modules are considered as non-volatile storage devices, as described in Security terms and definitions > Media.

Table 4-3: Types of media memory modules

Memory type	Location	Size	Content / Function	User modifiable
Solid-state drive (SSD) (removable)	Rear of the R&S FSW	Variable	• Operating system • Instrument firmware and firmware options with license keys • Instrument states and setups • Trace data • Limit lines, transducer tables • Screen images	Yes

5 Instrument sanitization procedure

5.1 Volatile memory

You can purge the volatile memory by following the procedure below. The sanitizing procedure complies to the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 3.

Removing power

To turn off and remove power

1. Turn off the R&S FSW.
2. Disconnect the power plug.

   Provided the instrument remains without power for at least five minutes, all volatile memory modules lose their contents, see [1].

5.2 Non-volatile memory

The non-volatile memories do not contain user data. Therefore no sanitization procedure is required.

5.3 Media

To remove the classified solid-state drive, perform the following steps:

1. Turn off the R&S FSW and disconnect the power plug.
2. Locate the SSD.

Figure 5-1: Location of the solid-state drive

3. Unscrew the two knurled screws.
4. Remove the solid-state drive from the R&S FSW.
5. Keep the solid-state drive under organizational control.

6 Operability outside the secured area

As the solid-state drive holds the operating system, the R&S FSW cannot be operated without the solid-state drive. For servicing and calibration, Rohde & Schwarz provides a separate solid-state drive (option R&S FSW-B18). This solid-state drive contains the operating system and required instrument data.

To establish the functionality outside the secured area:

1. Insert a second solid-state drive (option R&S FSW-B18).
   This solid-state drive enables the R&S FSW to start the operating system.
2. Turn on the R&S FSW.
3. Perform a self-alignment as described in Chapter 7, "Validity of instrument calibration after sanitization", on page 9 or Chapter 8.2, "Secure User Mode (R&S FSW-K33)", on page 10 if Secure User Mode (R&S FSW-K33) is enabled.

   The instrument is ready for use.

7 Validity of instrument calibration after sanitization

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

After exchanging the removable SSD, perform a self-alignment once:

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

1. Select the [SETUP] key.
2. Select the "Alignment" softkey.
3. Select "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.

8 Special security features

This section leads you to the information on how to use the security features to protect the R&S FSW from unauthorized access of classified information saved or displayed in the instrument.

The user manual is provided for download on the product page at www.rohde-schwarz.com/manual/FSW.

8.1 Considerations for USB interfaces

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 or write several Gbyte of data.

You can disable the write capability on the USB ports of the R&S FSW via a utility software. This utility software is available on the R&S FSW website https://www.rohde-schwarz.com/manual/r-s-fsw-instrument-security-manuals-gb1_78701-616615.html.

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

8.2 Secure User Mode (R&S FSW-K33)

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 FSW-K33, Security write protection of solid state drive) 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 FSW normally 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.

Securing Self Alignment Data when Secure User Mode is enabled

When the secure user mode (R&S FSW-K33) is enabled, the R&S FSW redirects the self alignment data to the volatile memory (SDRAM). The SDRAM memory loses its data when you power off the instrument.

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

To make sure that no self alignment data is lost, follow the instructions closely:

1. Deactivate the write protection of the SSD to allow the alignment data to be saved on the SSD. The write protection is disabled by deactivating the secure user mode (requires administrator login):
   Note: If you do not remove the write protection before, the self alignment data is lost when you power off the instrument. As a result, the measurement values can deviate later on.
   a) Select [SETUP] > "System Configuration".
   b) In the "Config" tab, select "Secure User Mode > Off".
      This change does not take effect until you have restarted the instrument.
   c) Reboot the R&S FSW.
2. Perform the self-alignment:
   a) Select [SETUP] > "Alignment".
   b) Select "Start Self Alignment".

   Once the system correction values have been calculated successfully, the R&S FSW prompts a message.

   The R&S FSW saves the self-alignment data on the SSD.

To reactivate the secure user mode:

1. Select [SETUP] > "System Configuration".
2. In the "Config" tab, select "Secure User Mode": "On".
3. Reboot the R&S FSW to apply the change.

Glossary

C

CFast: Compact Fast - compact flash mass memory device.

D

DRAM: Dynamic Random Access Memory.

H

HDD: Hard disk drive.

M

microSD: Micro Solid-state Drive - memory card.

S

SD: Solid-state drive - memory card.

SSD: ATA Solid-state drives (including PATA, SATA, eSATA, mSATA,...).

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