R&S®OSP
Open Switch and Control Platform
Instrument Security Procedures

1179467002
Version 01

ROHDE&SCHWARZ
Make ideas real

This document describes the types of memory and their use in the R&S®OSP base unit models.
While every effort has been made to ensure the accuracy of the information herein, it is provided without warranty. Design iteration and revisions may result in minor differences between the information provided here and your product.

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

1179.4670.02 | Version 01 | R&S®OSP

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

Contents

1 Overview

Securing important information is crucial in many applications.

In many cases, it is imperative that the R&S OSP instruments are used in a secured environment. 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 OSP.

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: R&S OSP models

Product name	Order number
R&S OSP220	1528.3105K02
R&S OSP230	1528.3105K03
R&S OSP320	1528.3111K02

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 is to keep physical media holding sensitive information 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. Media are user-accessible and retain data when you turn off power.

In the context of this document, 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 OSP 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	1 Gbyte	Temporary information storage for operating system and instrument firmware	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	every HW option module	256 byte	Board identification data	No
EEPROM	Main board	256 byte	Board identification data	No
EEPROM	Main board	256 byte	Device-specific	No
EEPROM	Main board	16 kbyte	MAC network configuration	No
EEPROM	Main board	2 kbit	EDID data for display	No
Flash	CPU board	64 kbyte	BIOS	No
Flash	Main board	256 Mbyte	Product options	No
Flash	Main board	256 Mbyte	FPGA configuration	No
microSD card	See Table 4-3			

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
microSD card	rear panel	16 Gbyte or more	Operating system, device configuration	yes
USB stick	front and/or panel	user defined	Instrument settings, optional	yes

5 Instrument sanitization procedure

If you remove the microSD card from the rear panel, the R&S OSP is left without operating system. Hence, the instrument is not useable after removing the microSD card.

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 4.

To turn off and remove power

1. Turn off the R&S OSP.
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.

If you are unsure about the security of the data stored on the microSD card, consider removing it before the R&S OSP leaves the secured area.

5.3 Media

You can sanitize the open switch and control platform by removing the microSD card and external USB storage devices.

To store all your configurations before sanitization

Prevent losing your path definitions and other configuration data by creating a backup as follows:

1. Turn on the R&S OSP.
2. Navigate to the "Backup Device" dialog:
   Access: "Configuration" > "General" > "Context Menu" > "Backup/Restore" > "Backup Device".
3. Connect a USB storage device to one of the front or rear USB ports.
4. In the "Device:" field, select this USB storage device.
5. In the "Filename:" field, specify a filename for your backup file.
6. Click "OK" in the top right corner of the dialog.

   The R&S OSP saves all configuration data in a backup file in the USB storage device.
7. Remove the USB storage device as described in the next procedure.
8. Keep the USB storage device under organizational control.

To remove USB sticks at the front or rear panel of the instrument

If one or more external USB storage devices (for example "USB sticks") are connected to the front or rear USB ports of the R&S OSP, proceed as follows to remove these USB storage devices:

1. Turn on the R&S OSP.
2. Navigate to a dialog that allows importing or exporting data from or to an external USB storage device.
   For example, navigate to "Configuration" > "General" > "Context Menu" > "Backup/Restore" > "Backup Device".
3. In the "Device:" field, select the USB storage device that you want to remove.
   For example, select a USB storage device with the <devicename> = `MY-USBSTICK`.
4. Click the eject button on the right-hand side of the "Device:" field.

   

   The firmware brings up a message to notify you that "The device '<devicename>' can now be safely removed."
5. Click "Close" to confirm this message.
6. Remove the USB storage device from its port.
7. If more USB storage devices are connected, repeat step 2 to step 6 for each device.

8. Keep the USB storage devices under organizational control.

To remove the microSD card at the rear panel of the instrument:

1. **NOTICE!** Do not remove the microSD card during operation as data can get lost. Turn off the R&S OSP.
2. Disconnect the power plug from the switch unit.
3. Disconnect any LAN, USB or D-Sub cable, if connected at the rear panel.
4. Remove the screws (labeled 1 in Figure 5-1) that fix the metal cover sheet (A or B).
5. Remove the metal cover sheet (A or B).
6. Remove the two screws (4) that fix the cap (3).
7. Remove the cap (3) from the microSD card slot.
8. To unlock the microSD card (5), carefully push it with your fingertip.
   The microSD card is released and pops out a little.
9. Remove the microSD card.
10. If you wish to insert a different microSD card, carefully push it in until it latches. Doing so, mind the orientation: angled edge to the front, contacts down. If you insert it in a wrong orientation, it cannot latch.
11. Reattach the cap (3) to cover the microSD card slot.
12. Fix the cap (3) by its two screws (4).
13. Reattach the the metal cover sheet (A or B) by its screws (1).
14. Keep the original microSD card under organizational control.

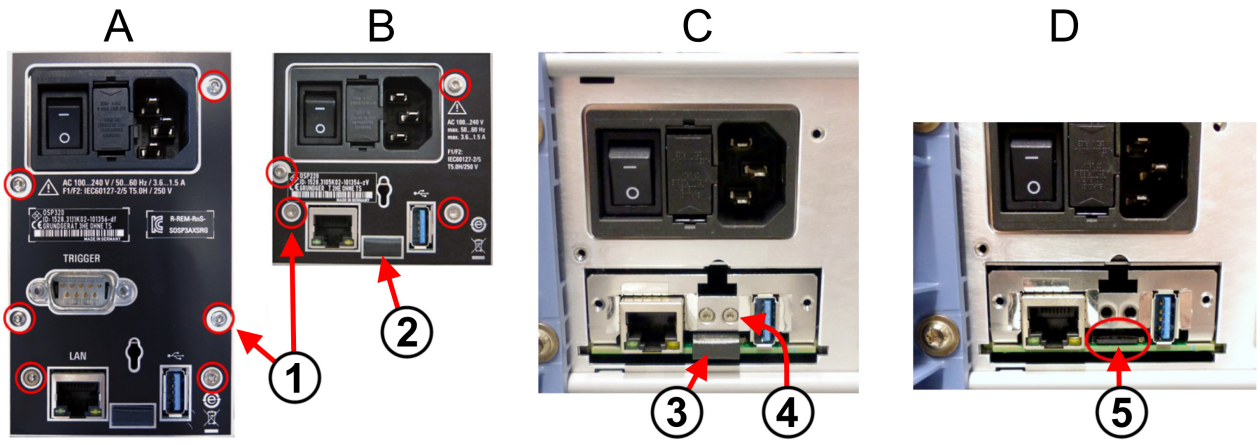

Figure 5-1: Removing the microSD card

A = Metal cover sheet of R&S OSP320
B = Metal cover sheet of R&S OSP220 and R&S OSP230
C = R&S OSP220, metal cover sheet removed
D = R&S OSP220, cap (3) removed

1 = Six or four screws (red circles) that fix the metal cover sheet
2 = Cap in metal cover sheet, protecting the microSD card
3 = Cap (= 2) must be removed to access the microSD card
4 = Two screws that fix the cap
5 = microSD card (red circle) in card slot

6 Functionality outside secured area

If you must restore the functionality of the R&S OSP on your premises, outside the secured area, contact Rohde & Schwarz service.

7 Recommended security settings

The following sections describe measures that protect from unauthorized access during operation, and procedures that enable you to remove user data before issuing the instrument outside the secure environment.

7.1 USB interfaces

There are no special requirements for R&S OSP USB ports to avoid unauthorized data access in a high-security location.

7.2 LAN interface

To protect the instrument against unauthorized data access in a high-security location, you can disconnect the R&S OSP from LAN and operate it locally.

7.3 Graphical user interface (GUI)

To protect the instrument against unauthorized personnel from using the GUI controls in the the front panel's touchscreen, you can set a "local lock-out" (LLO) remotely. To do so, enter "`&llo`" in the remote-control interface, as described in the user manual.

Glossary: Terminology for instrument security procedures

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,...).

Index

L

M

N

O

P

R

S

T

U

V