R&S®ZNB/ZNBT/ZNC/ZND
Vector Network Analyzer
Instrument Security Procedures

1175640302
Version 09

ROHDE&SCHWARZ
Make ideas real

This document describes the types of memory and their use in R&S®ZNB, ZNBT, R&S®ZNC, and R&S®ZND.
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.

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

1175.6403.02 | Version 09 | R&S®ZNB/ZNBT/ZNC/ZND

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

Contents

1 Overview....3
2 Instrument models covered....4
3 Security terms and definitions....5
4 Statement of volatility....6
5 Instrument sanitization procedure....8
6 Operability outside secured area....10
7 Validity of instrument calibration....11
8 Special security features....11
Glossary....12
Index....12

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 product.

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: Vector Network Analyzer models

Vector Network Analyzer	Order number
R&S ZNB4 - 2 port	1311.6010K22 (1st gen), 1334.3330K22 (2nd gen)
R&S ZNB4 - 4 port	1311.6010K24 (1st gen), 1334.3330K24 (2nd gen)
R&S ZNB8 - 2 port	1311.6010K42 (1st gen), 1334.3330K42 (2nd gen)
R&S ZNB8 - 4 port	1311.6010K44 (1st gen), 1334.3330K44 (2nd gen)
R&S ZNB20 - 2 port	1311.6010K62 (1st gen), 1334.3330K62 (2nd gen)
R&S ZNB20 - 4 port	1311.6010K64 (1st gen), 1334.3330K64 (2nd gen)
R&S ZNB26 - 2 port	1334.3330K63 (2nd gen)
R&S ZNB26 - 4 port	1334.3330K65 (2nd gen)
R&S ZNB40 - 2 port	1311.6010K72 (1st gen)
R&S ZNB40 - 2 port	1311.6010K82 (1st gen)
R&S ZNB40 - 4 port	1311.6010K84 (1st gen)
R&S ZNB43 - 2 port, 2.92 mm	1334.3330K92 (2nd gen)
R&S ZNB43 - 2 port, 2.4 mm	1334.3330K93 (2nd gen)
R&S ZNB43 - 4 port, 2.92 mm	1334.3330K94 (2nd gen)
R&S ZNB43 - 4 port, 2.4 mm	1334.3330K95 (2nd gen)
R&S ZNBT8 - up to 24 ports	1318.7006K24
R&S ZNBT20 - up to 24 ports	1332.9002K24, 1332.9002K64
R&S ZNBT26 - up to 24 ports	1332.9002K34
R&S ZNBT40 - up to 24 ports	1332.9002K44
R&S ZNC3	1311.6004K12
R&S ZND	1328.5170K92

3 Security terms and definitions

Terms defined in Guidelines for Media Sanitization

According to NIST Special Publication 800-88 [1]: "Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort." It defines the following categories of sanitization:

- **"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]

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 ZNB/ZNBT/ZNC/ZND 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.

This document uses the common notation kbyte, Mbyte and Gbyte for memory sizes, although the prefix multiplication factor is 1024.

4.1 Volatile memory

Volatile memory modules refer to 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	• **R&S ZNB:** 2 Gbyte or 8 Gbyte • **R&S ZNBT:** 8 Gbyte • **R&S ZNC:** 2 Gbyte or 4 Gbyte • **R&S ZND:** 4 Gbyte	Temporary information storage for operating system and instrument firmware	Yes

4.2 Non-volatile memory

Non-volatile memory modules refer to 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 assemblies	Up to 32 Mbyte	• Hardware information: – Serial number – Product options – Calibration correction data • BIOS	No
Flash (board assembly)	Board assemblies	Up to 32 Mbyte	FPGA configuration data	No

Each board assembly in the R&S ZNB/ZNBT/ZNC/ZND Vector Network Analyzer has either a serial EEPROM device **or** a Flash memory device. Both do not hold user data nor can the user access the storage.

4.3 Media

Media memory modules refer to 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
HDD or SSD	Removable system drive	128 to 500 Gbyte	• Operating system • Instrument firmware • Instrument states and setups • Limit lines • User calculation data • Trace data • Measurement results and screen images	Yes

The R&S ZNB/ZNBT/ZNC/ZND Vector Network Analyzer is equipped with a removable system drive (HDD or SDD).

The system drive can hold user data and is non-volatile. Hence, user data is not erased when power is removed from the instrument.

5 Instrument sanitization procedure

NOTICE

Risk of losing operability

The removable system drive holds the operating system. Removing it makes the instrument unusable.

We recommend that you keep a second non-classified system drive for use outside the secured area.

5.1 Volatile memory

You can purge the volatile memory by following the procedure below. The sanitization procedure complies with the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 5.

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

To turn off and remove power

1. Turn off the R&S ZNB/ZNBT/ZNC/ZND.
2. Disconnect the power plug.

   Leave the instrument powered off at least for 10 minutes to make sure that all volatile memory modules lose their contents, see [3].

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 system drive:

1. **NOTICE!** Do not remove the system drive during operation. Risk of data loss.

   Turn off the R&S ZNB/ZNBT/ZNC/ZND.
2. Locate the system drive at the rear of the instrument.

Figure 5-1: Location of the system drive for R&S ZNB (1st gen), R&S ZNBT, and R&S ZNC

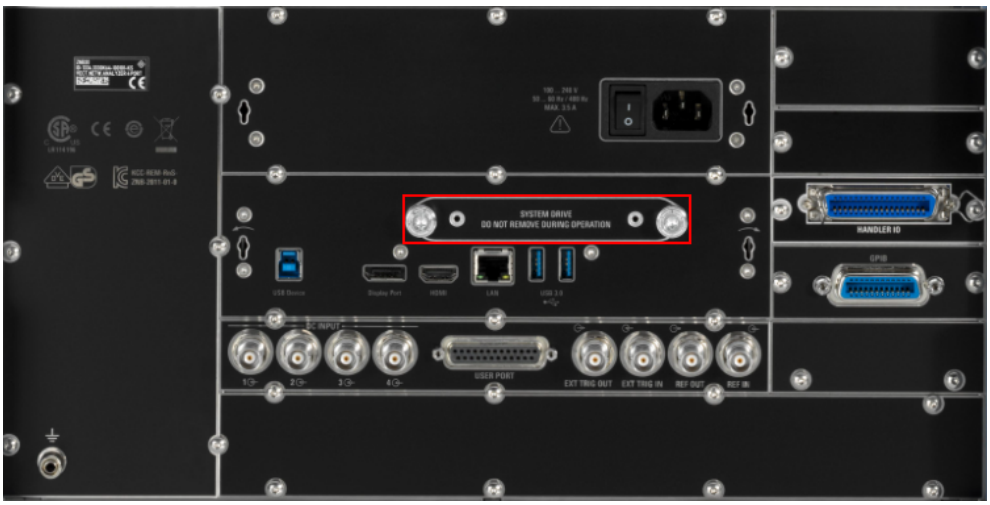

Figure 5-2: Location of the system drive for R&S ZNB (2nd gen)

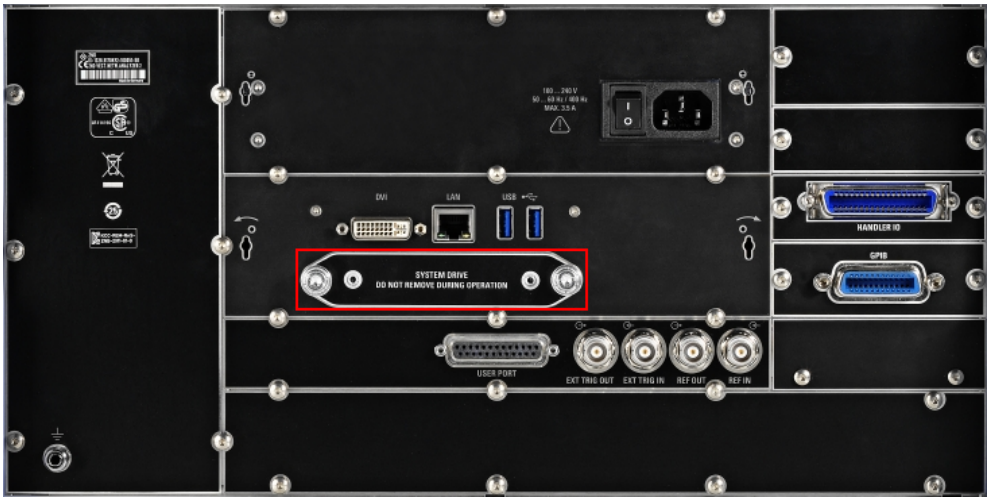

Figure 5-3: Location of the system drive for R&S ZND

3. Unscrew the two knurled screws.
4. Remove the system drive.
5. Keep the removed drive under organizational control.

6 Operability outside secured area

Once the Vector Network Analyzer is outside the secured area, installing a second non-classified removable system drive (without any user data) allows the Vector Network Analyzer to function properly for service or other needs (options R&S ZNB/ZNBT/ZNC/ZND-B19).

Prior to re-entering the secured area, the non-classified removable system drive (without the user data), is removed. When the Vector Network Analyzer is back within the secured area, the original classified removable system drive can be reinstalled.

- To hold classified user data in secure areas, use the removable system drive which comes with the instrument.
- To hold non-classified user data in non-secure areas, use a second removable system drive (R&S ZNB/ZNBT/ZNC/ZND-B19).

To restore operability outside the secured area

► Install a non-classified system drive (without any user data).

Enables the R&S ZNB/ZNBT/ZNC/ZND to start the operating system.

To return to the secured area

Before reentering the secured area:

► Remove the non-classified system drive, if necessary.

To restore operability inside secured area

1. Install the original (classified) system drive.
2. Connect the instrument to the power supply.

   The R&S ZNB/ZNBT/ZNC/ZND is ready for use.

7 Validity of instrument calibration

The non-volatile EEPROM is the only memory type used to hold permanent calibration correction data required to maintain the validity of the calibration. Because the sanitization procedure does not clear the non-volatile data, it does not affect the validity of the instrument's calibration.

8 Special security features

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

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/write several Gbyte of data.

Disabling USB ports for writing user data

You can disable the write capability of the instrument's USB ports via a "USB Write Protection Utility" software that is available for download on the Rohde & Schwarz Internet site. To disable the write capability, follow the instructions of the utility's Installation Manual.

8.2 Considerations for the user interface

The analyzer firmware allows you to mask all stimulus value occurrences at the graphical user interface (GUI), and to set a password for unmasking.

This is a pure GUI feature. It does not protect you from any kind of data readout via remote control.

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,...).

Index

C

Calibration validity
Sanitization procedure 11
Clear 5
Control of media 5

D

Destroy 5

G

Guideline definition 5

H

How to:
Establish operability inside secured area 11
Establish operability outside secured area 10
Remove system drive 8
Return to secured area 10
Sanitize media memory 8
Sanitize volatile memory 8

I

Instrument models 4
Instrument sanitization
Non-volatile memory 8

L

Literature
see References 4

M

Media
How to remove system drive 8
Memory types 7
Sanitization procedure 8
Terms and definitions 5
Memory types 6
Media 7
Non-volatile memory 7
Volatile memory 6

N

NIST 3
Non-volatile memory
Instrument sanitization 8
Memory types 6
Terms and definitions 5

O

Operability
Outside secured area 10
Operability outside secured area
How to restore 10
Outside secured area
Operability 10
Overview 3

P

Purge 5

R

References 4
Remove power
Sanitization procedure 8
Remove system drive 8
Restore operability inside secured area 11
Restore operability outside secured area 10
Return to secured area 10, 11

S

Sanitization 5, 8
Sanitization procedure
Calibration validity 11
Media 8
Non-volatile memory 8
Volatile memory 8
Special security features 11
USB interface 11
User interface 11
Statement of volatility 6

T

Terms and definitions 5
Clear 5
Control of media 5
Destroy 5

Media 5
Non-volatile memory 5
Purge 5
Sanitization 5
Volatile memory 5

U

USB interface
Security features 11
User interface
Security features 11

V

Volatile memory
Instrument sanitization 8
Memory types 6
Terms and definitions 5

Muehldorfstr. 15, 81671 Muenchen, Germany
Phone: +49 89 41 29 - 0
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®ZNB is indicated as R&S ZNB.