R&S®ZNA
Vector Network Analyzer
Instrument Security Procedures

1178982602
Version 02

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 ZNA.

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

Vector Network Analyzer, 2 ports, 26.5 GHz, 3.5 mm connectors	R&S ZNA26	1332.4500K22
Vector Network Analyzer, 4 ports, 26.5 GHz, 3.5 mm connectors	R&S ZNA26	1332.4500K24
Vector Network Analyzer, 2 ports, 43.5 GHz, 2.92 mm connectors	R&S ZNA43	1332.4500K42
Vector Network Analyzer, 4 ports, 43.5 GHz, 2.92 mm connectors	R&S ZNA43	1332.4500K44
Vector Network Analyzer, 2 ports, 43.5 GHz, 2.4 mm connectors	R&S ZNA43	1332.4500K43
Vector Network Analyzer, 4 ports, 43.5 GHz, 2.4 mm connectors	R&S ZNA43	1332.4500K45
Vector Network Analyzer, 2 ports, 50 GHz, 2.4 mm connectors	R&S ZNA50	1332.4500K52
Vector Network Analyzer, 4 ports, 50 GHz, 2.4 mm connectors	R&S ZNA50	1332.4500K54
Vector Network Analyzer, 2 ports, 67 GHz, 1.85 mm connectors	R&S ZNA67	1332.4500K62
Vector Network Analyzer, 4 ports, 67 GHz, 1.85 mm connectors	R&S ZNA67	1332.4500K64

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 in the R&S ZNA

The R&S ZNA 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
SRAM (Motherboard)	36 Mbit	Sweep control parameters	Volatile	Yes	Turn off instrument power

Memory type	**Size**	**Content**	**Volatility**	**User Data**	**Sanitization procedure**
Flash (Motherboard)	64 Mbyte	FPGA configuration file, Hardware information: ● Serial number ● Product options ● Instrument internal correction data	Non-volatile	No	None required (no user data)
EEPROM (board assembly)	256 bytes up to 1 Mbyte	Hardware information: ● Serial number ● Product options ● Instrument internal correction data	Non-volatile	No	None required (no user data)
Flash (CPU board)	8 Mbyte (IPC11/4)	BIOS	Non-volatile	No	None required (no user data)
Solid State Drive (SSD; removable system drive)	variable	● Operating system ● Instrument firmware ● Instrument states and setups ● Limit lines and transducer tables ● User calculation data ● User correction data ● Trace data ● Measurement results and screen images	Non-volatile	Yes	Remove system drive from instrument

4.1 Volatile Memory

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

4.2 Non-Volatile Memory

The R&S ZNA contains various non-volatile memories. Among these memories, only the removable system drive (a solid state drive) contains user data. All other non-volatile memories of the R&S ZNA are not a security concern.

Solid State Drive (Removable System Drive)

The R&S ZNA Vector Network Analyzer is equipped with a removable system drive (solid state drive).

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

To make sure that no user data is stored within the R&S ZNA, the system drive can be removed from the instrument.

The removable system drive addresses the needs of customers working in secured areas.

Sanitization procedure: Remove the system drive from the instrument.

5 Instrument Declassification

Before you can remove the instrument from a secured area (for example to perform service or calibration), all classified user data needs to be removed. You can declassify the Vector Network Analyzer R&S ZNA as follows:

1. Turn off the instrument and disconnect its power plug to sanitize the volatile memory.
2. Remove the classified removable system drive (containing user data).

Following these steps removes all user data from the R&S ZNA. It can now leave the secured area.

This declassification procedure meets the needs of customers working in secured areas.

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

Before reentering the secured area, the non-classified removable system drive 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, remove the instrument's removable system drive.
- To hold non-classified user data in non-secure areas, use an additional removable system drive (R&S ZNA-B19).

Validity of instrument calibration after declassification

The Flash (motherboard) and EEPROM are the only memory types holding permanent adjustment values that are required to maintain the validity of the instrument's calibration. Therefore, replacing one system drive of a R&S ZNA with another, does not affect the validity of its calibration.

6 Special Considerations for USB Ports

USB ports can pose a security risk in high-security environments. 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 ZNA via a utility software. This utility software is available on the R&S ZNA website https://www.rohde-schwarz.com/product/zna/.

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

ⓘ If the USB ports are disabled for USB memory devices, it is not possible to store any user characterization data on a calibration unit R&S ZN-Zxx.

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®ZNA is indicated as R&S ZNA.