

R&S®ZNH

Handheld Vector Network Analyzer Instrument Security Procedures



1334600002
Version 01

ROHDE & SCHWARZ
Make ideas real



This document describes the types of memory and their usage in the R&S®ZNH Handheld Vector Network Analyzer.

© 2021 Rohde & Schwarz GmbH & Co. KG

Mühlhofstr. 15, 81671 München, Germany

Phone: +49 89 41 29 - 0

Email: info@rohde-schwarz.com

Internet: www.rohde-schwarz.com

Subject to change – data without tolerance limits is not binding.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.

Trade names are trademarks of the owners.

1334.6000.02 | Version 01 | R&S®ZNH

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

Contents

1	Overview.....	5
2	Instrument Models Covered.....	6
3	Security Terms and Definitions.....	7
4	Statement of Volatility.....	9
4.1	Volatile Memory.....	9
4.2	Non-Volatile Memory.....	9
4.3	Media.....	10
5	Instrument Sanitization Procedure.....	11
5.1	Volatile Memory.....	11
5.2	Non-volatile Memory.....	11
6	Validity of Instrument Calibration after Sanitization.....	13
	Glossary: Terminology for Instrument Security Procedures.....	14
	Index.....	15

1 Overview

Securing important information is crucial in many applications.

In many cases, it is imperative that the R&S ZNH 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 ZNH.

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 ZNH models

Product name	Order number
R&S ZNH4	1321.1611.04
R&S ZNH8	1321.1611.08
R&S ZNH18	1321.1611.18
R&S ZNH26	1321.1611.26
R&S ZNH4	1321.1611.54, equivalent to 1321.1611.04
R&S ZNH8	1321.1611.58, equivalent to 1321.1611.08
R&S ZNH18	1321.1611.68, equivalent to 1321.1611.18
R&S ZNH26	1321.1611.76, equivalent to 1321.1611.26

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 ZNH 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 memory devices, as described in [Security Terms and Definitions > Volatile Memory](#). It requires power to retain data and when the power is turned off, all data is erased.

Table 4-1: Types of volatile memory

Memory type	Location	Size	Content	User data	Sanitization procedure
SDRAM	Mainboard	512 Mbyte	Temporary information storage for operating system and instrument firmware	Yes	Turn off instrument power and remove the battery. See Instrument Sanitization Procedure
SRAM	Frontboard (μ Controller internal)	4 kbyte	Temporary information storage for power-up / power-down firmware.	No	

4.2 Non-Volatile Memory

Non-volatile memory modules are considered as non-accessible internal memory devices, as described in [Security Terms and Definitions > Non-volatile Memory](#). It does not require power to maintain the stored data.

Table 4-2: Types of non-volatile memory

Memory type	Location	Size	Content	User data	Sanitization procedure
Flash	Frontboard (μ Controller internal)	32 kbyte	Power-up / power-down firmware	No	None required (no user data)
Flash	Mainboard	128 Mbyte	<ul style="list-style-type: none"> • Operating system • Instrument firmware • Boot code • Calibration correction data, device options and serial number • User data and instrument settings 	Yes	See Instrument Sanitization Procedure

4.3 Media

Media are considered as non-volatile memory devices, as described in [Security Terms and Definitions > Media](#).

Table 4-3: Types of media memory modules

Memory type	Location	Size	Content	User data	Sanitization procedure
USB	Instrument top view	n.a.	n.a.	Yes	Remove memory device and keep it under organizational control. See Instrument Sanitization Procedure
microSD	Instrument rear view. Behind the battery compartment.	n.a.	n.a.	Yes	

5 Instrument Sanitization Procedure

5.1 Volatile Memory

Removing power

1. Turn off the R&S ZNH.
2. Remove the battery.

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 Flash does not lose its contents when power is removed. It can contain user data.

Sanitizing the non-volatile memory

The Flash is **cleared** by executing the sanitizing procedure provided on the instrument. The sanitizing procedure complies to the definition of NIST [1], see "[Terms defined in Guidelines for Media Sanitization](#)" on page 7.

1. **NOTICE!** Risk of loosing data. The sanitization procedure clears all user data and resets the instrument.
Back up all data you want to keep.
2. Remove all media:
 - a) Disconnect USB mass memory.
 - b) Remove microSD card.
For information on how to proceed, see the corresponding instructions in the user manual of the R&S ZNH.
3. Keep the media memory devices under organizational control.
4. **NOTICE!** Risk of instrument damage when interrupting the sanitizing procedure. Do not turn off or disconnect the R&S ZNH from the mains while the sanitizing procedure is running.
Wait until the instrument confirms the completed sanitizing.
To activate the sanitizing procedure, press and hold the [PRESET] and [F5] keys while switching on the instrument.
After a few seconds, the sanitizing procedure starts.

The sanitizing procedure takes approximately 8 minutes, indicated by the message "Secure Formatting Flash, please wait!" on the screen.

When completed, the instrument reboots automatically.

6 Validity of Instrument Calibration after Sanitization

The validity of the R&S ZNH handheld vector network analyzer's calibration is maintained throughout the sanitization.

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

C

Calibration validity	
Instrument sanitization	13
Clear	7
Control of media	7

D

Destroy	7
---------------	---

G

Guideline definition	7
----------------------------	---

I

Instrument models	6
Instrument sanitization	
Calibration validity	13
Non-volatile memory	11
Volatile memory	11
Instrument sanitization procedure	
Volatile memory	11

L

Literature	
see References	5

M

Media	
Memory types	10
Remove	11
Terms and definitions	8
Memory types	9
Media	10
Non-volatile memory	9
Volatile memory	9

N

NIST	5
Non-volatile memory	
Instrument sanitization	11
Memory types	9
Sanitization procedure	11
Terms and definitions	7

O

Overview	5
----------------	---

P

Purge	7
-------------	---

R

References	5
Remove power	
Sanitization procedure	11

S

Sanitization	7
Sanitization procedure	
Remove power	11
Sanitize internal memory	11
Statement of volatility	9

T

Terms and definitions	7
Clear	7
Control of media	7
Destroy	7
Media	8
Non-volatile memory	7
Purge	7
Sanitization	7
Volatile memory	7

V

Volatile memory	
Instrument sanitization	11
Memory types	9
Terms and definitions	7