R&S®ZN-Z5x, R&S®ZN-Z15x, R&S®ZN-ZE1xx Calibration Units Instrument Security Procedures

1179039702
Version 03

ROHDE&SCHWARZ
Make ideas real

This document describes the types of memory and their use in the calibration units R&S®ZN-Z5x, R&S®ZN-Z150, R&S®ZN-Z151, R&S®ZN-Z152, R&S®ZN-Z153, R&S®ZN-Z156, and R&S®ZN-ZE1xx.

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

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

1179.0397.02 | Version 03 | R&S®ZN-Z5x, R&S®ZN-Z15x, R&S®ZN-ZE1xx

Throughout this document, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®ZN-Z151 is indicated as R&S ZN-Z151.

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 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: R&S ZN-Z5x, R&S ZN-Z15x, R&S ZN-ZE1xx models

Product	Ports	Frequency range	Order number
R&S ZN-Z5x			
R&S®ZN-Z50 calibration unit	2 ports, 3.5 mm (f)	9 kHz to 9 GHz	1335.6904.30
		9 kHz to 26.5 GHz	1335.6904.32
R&S®ZN-Z51 calibration unit	4 ports, 3.5 mm (f)	100 kHz to 8.5 GHz	1319.5507.34
	2 ports, 3.5 mm (f)		1319.5507.32
	4 ports, N (f)		1319.5507.74
	2 ports, N (f)		1319.5507.72
R&S®ZN-Z52 calibration unit	4 ports, 3.5 mm (f)	100 kHz to 26.5 GHz	1335.6991.30
R&S®ZN-Z53 calibration unit	2 ports, 3.5 mm (f)	100 kHz to 26.5 GHz	1335.7046.32
	2 ports, type N (f)	100 kHz to 18 GHz	1335.7046.72
R&S®ZN-Z54 calibration unit	2 ports, 2.92 mm (f)	9 kHz to 40 GHz[1)]	1335.7117.92
R&S®ZN-Z55 calibration unit	2 ports, 2.4 mm (f)	9 kHz to 50 GHz	1335.7181.42
R&S ZN-Z15x			
R&S®ZN-Z150 calibration unit	2 ports, N (f)	5 kHz to 6 GHz	1335.6710.72
R&S®ZN-Z151 calibration unit	2 ports, SMA (f)	100 kHz to 8.5 GHz	1317.9134.32
	2 ports, N (f)		1317.9134.72
R&S®ZN-Z152 calibration unit	6 ports, SMA (f)	100 kHz to 8.5 GHz	1319.6003.36
R&S®ZN-Z153 calibration unit	4 ports, SMA (f)	100 kHz to 8.5 GHz	1319.6178.34
R&S®ZN-Z156 calibration unit	2 ports, 1.85 mm (f)	5 GHz to 67 GHz	1332.7239.02
		10 MHz to 67 GHz	1332.7239.03
R&S ZN-ZE1xx			
R&S®ZN-ZE104 calibration unit	2 ports[2)]	5 kHz to 4.5 GHz	1350.8040K04
R&S®ZN-ZE109 calibration unit	2 ports[2)]	5 kHz to 9 GHz	1350.8040K09

Product	Ports	Frequency range	Order number
R&S®ZN-ZE118 calibration unit	2 ports[2)]	5 kHz to 18 GHz	1350.8040K18
R&S®ZN-ZE126 calibration unit	2 ports[2)]	5 kHz to 26.5 GHz	1350.8040K26
[1)] characterized up to 43.5 GHz			
[2)] The R&S ZN-ZE1xx models are equipped with two of the following port options: ● R&S®ZN-ZE1-B170, N (f), port 1 ● R&S®ZN-ZE1-B171, N (m), port 1 ● R&S®ZN-ZE1-B270, N (f), port 2 ● R&S®ZN-ZE1-B271, N (m), port 2 ● R&S®ZN-ZE1-B130, 3.5 mm (f), port 1 ● R&S®ZN-ZE1-B131, 3.5 mm (m), port 1 ● R&S®ZN-ZE1-B230, 3.5 mm (f), port 2 ● R&S®ZN-ZE1-B231, 3.5 mm (m), port 2			

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 ZN-Z5x, R&S ZN-Z15x, R&S ZN-ZE1xx contain 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
SRAM	µController	52 kbyte	Temporary information storage for 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
Flash	µController	2x128 kbyte	● Firmware	No
Flash	On-board flash memory	128 Mbyte	● Product identification data (serial number, hardware info) ● Calibration data ● Factory characterization data ● User characterization data generated by the analyzer firmware	Yes

4.3 Media

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

R&S ZN-Z150, R&S ZN-Z151 and R&S ZN-Z156 are not equipped with a microSD card slot. Hence, they do not have a media memory.

Table 4-3: Types of media memory modules

Memory type	Location	Size	Content / Function	User modifiable
microSD card (removable)	see Location of the microSD card slot	1 Gbyte (R&S ZN-Z5x, R&S ZN-Z15x)	● User data ● User characterization data generated by the analyzer firmware	Yes
		8 Gbyte (R&S ZN-ZE1xx)		

5 Instrument sanitization procedure

5.1 Volatile memory

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

To remove power

► Disconnect the USB connection cable.

Provided the instrument remains without power for at least 10 minutes, all volatile memory modules lose their contents, see [3].

5.2 Non-volatile memory

You can clear/purge the non-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.

To sanitize the non-volatile memory

Risk of losing data

The sanitization procedure clears/purges all user characterization data.

1. Connect the calibration unit to the network analyzer.
2. Access the characterization wizard of the network analyzer.
3. Select the calibration unit from the list.
4. Use one of the following functions to delete user characterization data from the selected calibration unit:
   - Use the "Delete" function to clear the user characterizations from the non-volatile memory.
   - Use the "Sanitize" function to purge all user characterizations from the non-volatile memory.

   Note: The "Sanitize" function is available on R&S ZVA, R&S ZVB and R&S ZVT only. These network analyzers do not support calibration units R&S ZN-ZE1xx.

5.3 Media

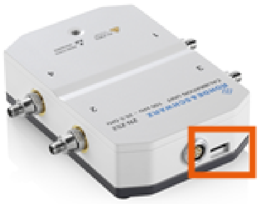
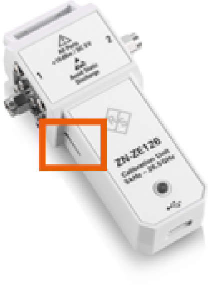
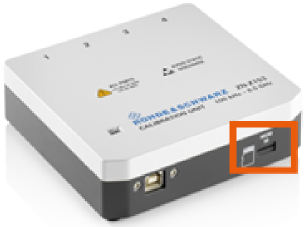
R&S ZN-Z150, R&S ZN-Z151 and R&S ZN-Z156 are not equipped with a microSD card slot. Hence, they do not require this kind of instrument declassification.

To remove the microSD card:

1. **NOTICE!** Do not remove the microSD card during operation. It can lose data.

   Power off the calibration unit by disconnecting the USB.
2. Remove the microSD card at the microSD card slot of the instrument.

Table 5-1: Location of the microSD card slot

R&S ZN-Z5x	R&S ZN-ZE1xx	ZN-Z152 and ZN-Z153
		

3. Keep the microSD card under organizational control.

6 Operability outside secured area

The sanitization does not affect the functionality of the R&S ZN-Z5x, R&S ZN-Z15x, R&S ZN-ZE1xx calibration unit. The instrument works properly after sanitization.

When the calibration unit is back within the secured area, the original classified removable microSD card can be reinstalled.

7 Validity of instrument calibration

The *Flash* is the only memory type used to hold permanent adjustment values required to maintain the validity of the calibration unit's calibration. Therefore, the sanitization procedure 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 of the network analyzer to protect the R&S ZN-Z5x, R&S ZN-Z15x, R&S ZN-ZE1xx from unauthorized access of classified information saved in the instrument.

8.1 Considerations for saving user characterization data

Current Rohde&Schwarz desktop network analyzers allow you to create user characterizations of your calibration unit. For calibration units with microSD card slot, the characterization data can be written to the inserted microSD card instead of the internal flash memory.

See Recommended security settings > Saving user characterization data.

9 Recommended security settings

Basically, see the user manuals of your network analyzer models for the security concept of the calibration unit, including instructions on how to select where to save user characterization data.

The user manuals of the network analyzers are provided for download on their product pages at www.rohde-schwarz.com.

The following section describes measures that protect user characterization data before issuing the instrument outside the secure environment.

9.1 Saving user characterization data

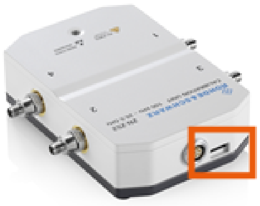
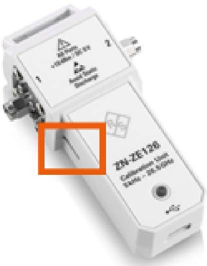
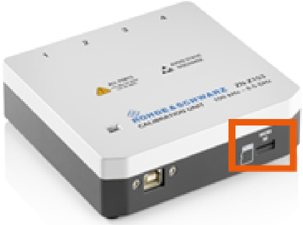
The R&S ZN-Z150, R&S ZN-Z151 and R&S ZN-Z156 are not equipped with a microSD card slot. Hence, the user characterization data is always saved on the internal flash memory.

To save user characterization data on a microSD card

You can save user characterization data on a microSD card instead of the calibration unit's internal flash memory.

1. Insert a microSD card into the microSD card slot of the instrument.

Table 9-1: Location of the microSD card slot

R&S ZN-Z5x	R&S ZN-ZE1xx	ZN-Z152 and ZN-Z153
		

2. Connect the calibration unit to the network analyzer.

3. Access the characterization wizard of the network analyzer.

4. Activate the checkbox when saving the characterization data.

   Tip: If the characterized calibration unit does not have an SD card slot, the checkbox is hidden. If the calibration unit has an SD card slot but the SD card is not accessible, the checkbox is grayed out.

   The characterization data is saved on the microSD card.