R&S®ZN-Z8x
Switch Matrix
Instrument Security Procedures

ROHDE&SCHWARZ

Make ideas real

This document describes the types of memory and their use in the R&S®ZN-Z8x switch matrices. 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.

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-Z8x models

Product name	Order number
R&S ZN-Z84 - 8.5 GHz, 6 to 24 ports	1319.4500K02
R&S ZN-Z85 - 20 GHz, 6 to 12 ports	1326.4777K03
R&S ZN-Z86 - 26.5 GHz 6 to 24 ports	1351.2216K02
R&S ZN-Z86X - 26.5 GHz, 6 to 24 ports	1351.2222K02

The number of ports can be increased to 12, 18 or 24 by means of the following extension ports:

- R&S®ZN-Z84-B22 Additional Ports 7-12 (2 VNA Ports) 1319.4969.22
- R&S®ZN-Z84-B24 Additional ports 7-12 (4 VNA Ports) 1319.4969.24
- R&S®ZN-Z84-B32 Additional ports 13-18 (2 VNA Ports) 1319.4969.32
- R&S®ZN-Z84-B34 Additional ports 13-18 (4 VNA Ports) 1319.4969.34
- R&S®ZN-Z84-B42 Additional ports 19-24 (2 VNA Ports) 1319.4969.42
- R&S®ZN-Z84-B44 Additional ports 19-24 (4 VNA Ports) 1319.4969.44
- R&S®ZN-Z85-B24 Additional ports 7-12 (4 VNA Ports) 1326.4831.26
- R&S®ZN-Z86-B22 "Additional ports 7–12 (2 VNA ports)", order no. 1351.2900.22
- R&S®ZN-Z86-B24 "Additional ports 7–12 (4 VNA ports)", order no. 1351.2900.24
- R&S®ZN-Z86-B32 "Additional ports 13–18 (2 VNA ports)", order no. 1351.2900.32
- R&S®ZN-Z86-B34 "Additional ports 13–18 (4 VNA ports)", order no. 1351.2900.34
- R&S®ZN-Z86-B42 "Additional ports 19–24 (2 VNA ports)", order no. 1351.2900.42
- R&S®ZN-Z86-B44 "Additional ports 19–24 (4 VNA ports)", order no. 1351.2900.44
- R&S®ZN-Z86X-B24 "ports 1-12 (4 VNA ports)", order no. 1351.2222.24
- R&S®ZN-Z86X-B44 "ports 1-24 (4 VNA ports)", order no. 1351.2222.44

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 ZN-Z8x switch matrix 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
Microcontroller RAM	Mainboard	100 kbyte	Temporary information storage for CPU operation	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
Microcontroller Flash	Mainboard	512 kbyte	Instrument firmware	No
EEPROM	Mainboard	4 Mbyte	• Hardware information: – Serial number – Product options – Calibration correction data	No
Flash	Mainboard	16 Mbyte	Not used for ZN-Z8x switch matrix	No

4.3 Media

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

The product R&S ZN-Z8x does not contain media.

5 Instrument sanitization procedure

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 4.

ⓘ 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 ZN-Z8x switch matrix.

2. Disconnect the power plug or USB.

    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

The R&S ZN-Z8x does not contain media memory modules. Therefore, no sanitization procedure is required.

6 Operability outside secured area

The sanitization does not affect the functionality of the R&S ZN-Z8x switch matrix. The instrument works properly after sanitization.

7 Validity of instrument calibration

The validity of the R&S ZN-Z8x switch matrix's calibration is maintained throughout the sanitization.