R&S®RT-Z
Oscilloscope Probes
Instrument Security Procedures

1179048002
Version 01

ROHDE&SCHWARZ
Make ideas real

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

1179.0480.02 | Version 01 | R&S®RT-Z

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

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 RT-Z.

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: Probes models

Product name	Order number
R&S RT-ZC05B	1409.8204.02
R&S RT-ZC10B	1409.8210.02
R&S RT-ZC15B	1409.8227.02
R&S RT-ZC20B	1409.8233.02
R&S RT-ZD10	1410.4715.02
R&S RT-ZD20	1410.4409.02
R&S RT-ZD30	1410.4609.02
R&S RT-ZD40	1410.5205.02
R&S RT-ZHD07	1800.2307.02
R&S RT-ZHD15	1800.2107.02
R&S RT-ZHD16	1800.2207.02
R&S RT-ZHD60	1800.2007.02
R&S RT-ZM15	1800.4700.02
R&S RT-ZM30	1419.3005.02
R&S RT-ZM60	1419.3105.02
R&S RT-ZM90	1419.3205.02
R&S RT-ZM130	1800.4500.02
R&S RT-ZM160	1800.4600.02
R&S RT-ZPR20	1800.5006.02
R&S RT-ZPR40	1800.5406.02
R&S RT-ZS10	1410.4080.02
R&S RT-ZS10E	1418.7007.02
R&S RT-ZS20	1410.3502.02
R&S RT-ZS30	1410.4309.02
R&S RT-ZS60	1418.7307.02

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 RT-Z 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

The R&S RT-Z do not contain volatile memory modules.

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 4-1: Types of non-volatile memory

Memory type	Location	Size	Content / Function	User modifiable
For all probes: Flash	µController	256 kbyte	• Probe firmware • Calibration data • For R&S RT-ZC probes: zero error	No
For R&S RT-ZHD probes only: Flash	µController	64 kbyte	• Probe firmware	No
For R&S RT-ZM probes only: Serial	Probe board	64 Mbit	• Calibration data	No

4.3 Media

The R&S RT-Z probes do not contain media, as defined in Security terms and definitions > Media.

5 Instrument sanitization procedure

The R&S RT-Z probes contain no volatile memory modules. The non-volatile memory modules do not contain user data. Therefore no sanitization procedure is required.

6 Validity of instrument calibration

The R&S RT-Z probes require no sanitization. Therefore the validity of the probe's calibration is not affected.