

R&S®MXO 4 Series

Oscilloscope

Instrument Security Procedures



1335550802
Version 01

ROHDE & SCHWARZ
Make ideas real



This document describes the types of memory and their use in the R&S®MXO 4 oscilloscope. 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.

© 2023 Rohde & Schwarz GmbH & Co. KG
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.
R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.
Trade names are trademarks of the owners.

1335.5508.02 | Version 01 | R&S®MXO 4 Series

Throughout this document, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®MXO 4 is indicated as R&S MXO 4 .

Contents

1 Overview	3
2 Instrument models covered	4
3 Security terms and definitions	4
4 Statement of volatility	5
5 Instrument sanitization procedure	7
6 Operability outside secured area	9
7 Validity of instrument calibration	9
Glossary	9

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 MXO 4 models

Product name	Order number
R&S MXO 4	1335.5050.04

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 MXO 4 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
SDRAM/DDR4	Mainboard	4 GByte	Temporary information storage for operating system and instrument firmware	Yes
SDRAM/DDR4	Mainboard	1 GByte	Waveform generator data	Yes
SRAM	Mainboard	16 kByte	Operating system	No
SDRAM/DDR4	Mainboard	≥ 7 GByte	<ul style="list-style-type: none"> Waveform data Measurement data 	Yes
SRAM	Front panel board	16 kByte	Operating system	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	Mainboard	128 kbyte	Boot code	No
Flash	Mainboard	≥ 16 Gbyte	<ul style="list-style-type: none"> Operating system and instrument firmware Firmware options and applications Instrument states and setups Waveform data Measurement results and screen images 	Yes
EEPROM	Mainboard	256 kbit	<ul style="list-style-type: none"> Product identification data Product options 	No
Flash	Front panel board	128 kbyte	Boot code	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 MXO 4 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 R&S MXO 4.
2. Disconnect the power plug.

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

You can [clear](#) 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 4.

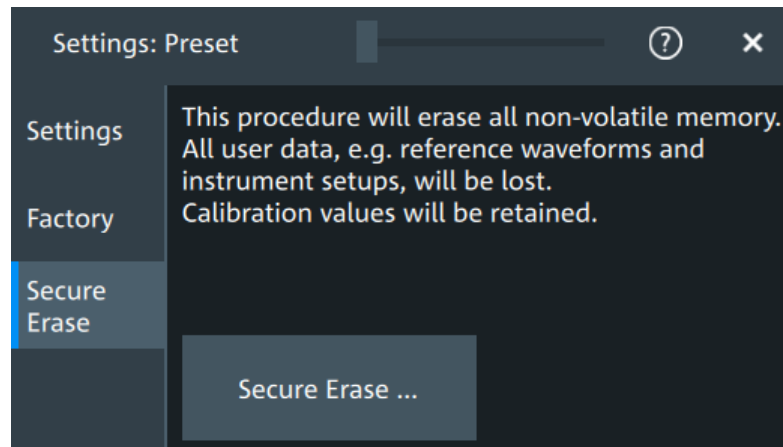
To sanitize the non-volatile memory



Risk of losing data

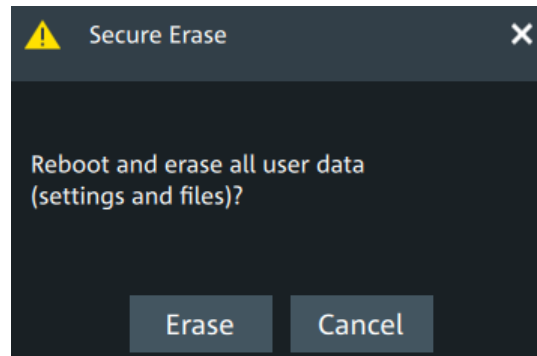
The sanitization procedure [clears](#) all user data and resets the instrument.

1. Back up all data you want to keep.
2. Open "Menu" > "Settings" > "Preset" > "Secure Erase".



3. Tap "Secure Erase".

A message box opens.



4. To start the secure erase procedure, tap "Erase".
All user data is removed and the factory default settings are restored.

NOTICE

Risk of instrument failure

Do not turn off the instrument during the Secure Erase process.

Turning off the instrument during the Secure Erase process might lead to a failure of the data partition mounting. In this case the instrument might not function properly and might need to be send for servicing.

5.3 Media

The R&S MXO 4 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 MXO 4 oscilloscope. The instrument works properly after sanitization.

7 Validity of instrument calibration

The validity of the R&S MXO 4 oscilloscope's calibration is maintained throughout the sanitization.

Glossary

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,...).