R&S®NGL200/NGM200
Power Supply Series
Instrument Security Procedures

3662972902
Version 02

ROHDE&SCHWARZ
Make ideas real

This document describes the types of memory and their use in the power supply series.
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

3662.9729.02 | Version 02 | R&S®NGL200/NGM200

Throughout this document, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®NGL200, R&S®NGM200 are indicated as R&S NGL/NGM.

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
5 Instrument sanitization procedure 11
5.1 Volatile Memory 11
5.2 Non-volatile memory 11
6 Operability outside secured area 13
7 Validity of Instrument calibration 14
8 Special security features 15
8.1 Considerations for LAN interfaces 15
9 Recommended security settings 16
9.1 LAN interfaces and services 16
Glossary 17
Index 18

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 NGL/NGM models

Product name	Order number
R&S®NGL201	3638.3376.02
R&S®NGL202	3638.3376.03
R&S®NGM201	3638.4472.02
R&S®NGM202	3638.4472.03

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 NGL/NGM 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
SRAM	Front controller board	-	Operating data	No
DDR3 SDRAM	Front controller board MPU One per channel	2 x 2 Gbit	Temporary information storage for: • Operating system • Instrument firmware • User and program data	No
SRAM	Channel-board One per channel	32 kbyte	Channel operating data	No

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
NAND Flash	Front controller board	4 Gbyte	• Board identification data • Firmware • Board internal correction data • Instrument settings and setups • User data	Yes
Flash	Channel-board MCU One per channel	• 256 kbyte • 3 kbyte boot	• Board internal correction • Bootloader	No
EEPROM	Channel-board MCU	32 kbit	• User data • Board internal correction data	No

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 7.

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. Sanitize the non-volatile memory as described in procedure Chapter 5.2, "Non-volatile memory", on page 11.
2. Turn off the R&S NGL/NGM power supply.
3. 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 7.

Sanitization is performed by means of a factory reset.

To execute a factory reset

1. **NOTICE!** Risk of losing data. The factory reset clears all user data and resets the instrument.

   Back up all data you want to keep.
2. If connected, disconnect the external USB mass memory.
3. Keep the media memory devices under organizational control.
4. **NOTICE!** Risk of instrument damage when interrupting the factory reset procedure. Do not turn off or disconnect the R&S NGL/NGM from the mains while the factory reset procedure is running.
   Wait until the instrument confirms the completed factory reset procedure.

To reset the instrument to factory default, press the [Menu] key on the front panel of the R&S NGL/NGM.

5. Select "Device" > "Reset" menu item.
6. Select "Yes" to proceed when prompted to reset all settings to factory defaults.
7. Wait for the "Device reset" message to appear at the top left corner of the screen.

   All user data will be removed and factory default settings restored.

6 Operability outside secured area

The sanitization does not affect the functionality of the R&S NGL/NGM power supply series. The instrument works properly after sanitization.

7 Validity of Instrument calibration

The validity of the R&S NGL/NGM power supply series's calibration is maintained throughout the sanitization.

8 Special security features

This section leads you to the information on how to use the security features to protect the R&S NGL/NGM from unauthorized access of classified information saved or displayed in the instrument.

8.1 Considerations for LAN interfaces

In a LAN, the interface can pose a security risk due to unauthorized data access during operation.

See Chapter 9, "Recommended security settings", on page 16.

9 Recommended security settings

Basically, see the user manual for the security concept of the R&S NGL/NGM, including instructions on how to prevent unauthorized access.

The user manual is provided for download on the product page at www.rohde-schwarz.com/manual/ngl200 and www.rohde-schwarz.com/manual/ngm200.

The following sections describe measures that protect from unauthorized access during operation, and procedures that enable you to remove user data before issuing the instrument outside the secure environment.

9.1 LAN interfaces and services

To protect the instrument against unauthorized data access in a high-security location, use it at local workplaces and connect it only to secured networks (LAN).

See the user manual for details.

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,...).

Index

C

Calibration validity
  Instrument sanitization 14
Clear 7
Control of media 7

D

Destroy 7

G

Guideline definition 7

H

How to:
  Sanitize non-volatile memory 11
  Sanitize volatile memory 11

I

Instrument models 6
Instrument sanitization
  Calibration validity 14
  Non-volatile memory 11
  Volatile memory 11

L

LAN interface
  Recommended security settings 16
  Security features 15
Literature
  see References 5

M

Media
  Terms and definitions 7
Memory types 9
  Non-volatile memory 10
  Volatile memory 9

N

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

O

Operability
  Outside secured area 13
Outside secured area
  Operability 13
Overview 5

P

Purge 7

R

Recommended security settings 16
  LAN interface 16
References 5
Remove power
  Sanitization procedure 11

S

Sanitization 7, 11
Sanitization procedure
  Volatile memory 11
Special security features 15
  LAN interface 15
Statement of volatility 9

T

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

V

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