R&S®LCX Series
LCR Meter
Instrument Security Procedures

1179572402
Version 01

ROHDE&SCHWARZ
Make ideas real

This document describes the types of memory and their use in instruments of the R&S®LCX 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

1179.5724.02 | Version 01 | R&S®LCX Series

Throughout the document, the products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®LCX is indicated as R&S LCX. R&S LCX refers to the LCR meter of the R&S LCX series.

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 LCX.

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 LCX models

Product name	Order number
R&S LCR100	3629.8856.02
R&S LCR200	3629.8856.03

3 Security terms and definitions

Terms defined in Guidelines for Media Sanitization

" NIST Special Publication 800-88 "[1]

- **"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]

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

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 LCX 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

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
OCRAM	Main processor on front controller board	128 kbyte	Boot code	No
TCMU/TCML		64 kbyte	Temporary information storage for instrument firmware	Yes
SDRAM	Front controller board	512 Mbyte	Temporary information storage for operating system and 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
EEPROM	Front controller board	4 kbit	Instrument identification data • Serial number • Software option licenses	No
Flash	Main board	32 Mbit	Calibration data	No
Flash, partitioned	Front controller board	2 Gbyte	See details of the partitions:	Yes
• partition 1		16 Mbyte	• Bootloader	No
• partition 2		512 Mbyte	• Operating system • Main application • Third-party applications and libraries	No
• partition 3		1 Gbyte	• User data – Settings – Storage – etc.	Yes

4.3 Media

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

The R&S LCX has no media memory modules installed.

5 Instrument sanitization procedure

5.1 Volatile memory

You can clear 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.

To turn off and remove power

1. Turn off the R&S LCX.
2. Disconnect the power plug.

   Provided the instrument remains without power for at least five minutes, all volatile memory modules lose their contents.

5.2 Non-volatile memory

You can clear the non-volatile memory using remote control commands as described in the procedure To sanitize the non-volatile memory remotely. 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 remotely

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

   Back up all data you want to keep.
2. Connect the instrument in a LAN, over USB or the GPIB interface (R&S NG-B105) to a controller device.
3. Start a controller application program on the controller.
4. Send the following remote I/O command sequence to the instrument:
   ```
   SERVice:UNLock 1234
   SERVice:SECure:ERASe
   ```
   The procedure "Sanitize internal memory" starts. The application indicates the currently performed action and its progress.

   After sanitization, the R&S LCX restores factory defaults and the network configuration.

5.3 Media

Instruments of the R&S LCX series do 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 LCX.

Thus the operability of the instrument is maintained after sanitization.

7 Validity of instrument calibration

The validity of the R&S LCX's calibration is maintained throughout the sanitization.