R&S®SMCV100B
Vector Signal Generator
Instrument Security Procedures

1179255402
Version 01

ROHDE&SCHWARZ
Make ideas real

This document describes the types of memory and their usage in the R&S®SMCV100B Vector Signal Generator.

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

1179.2554.02 | Version 01 | R&S®SMCV100B

Throughout this document, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®SMCV100B is indicated as R&S SMCV100B.

1 Overview

Securing important information is crucial in many applications.

In many cases, it is imperative that the R&S SMCV100B instruments are used in a secured environment. 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 SMCV100B.

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.

2 Instrument Models Covered

Table 2-1: R&S SMCV100B models

Product name	Order number
R&S SMCV100B	1432.7000K02

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 is to keep physical media holding sensitive information 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. The volatile memory is not a security concern.

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. Media are user-accessible and retain data when you turn off power.

In the context of this document, 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 SMCV100B 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 are considered as non-accessible internal memory devices, as described in "Volatile memory" on page 5.

Table 4-1: Types of volatile memory

Memory type	Location	Size	Content	User data	Sanitization procedure
SDRAM	IPS3	8 Gbyte	Temporary information storage for operating system and instrument firmware, or RAM disk for user data	yes	Turn off instrument power
SDRAM	BBCV	4 Gbit	Not used	n.a.	
SDRAM	BBCV	8 Gbyte	Temporary information storage for arbitrary waveforms and TS generator files	yes	
SRAM	BBCV (µController)	48 kbyte	Temporary storage of µController data	yes	
SRAM	RFCV (µController)	48 kbyte	Temporary storage of µController data	yes	
SRAM	FrontCV (µController)	48 kbyte	Temporary storage of µController data	yes	

4.2 Non-Volatile Memory

Non-volatile memory modules are considered as non-accessible internal memory devices, as described in "Non-volatile memory" on page 5.

Table 4-2: Types of non-volatile memory

Memory type	Location	Size	Content	User data	Sanitization procedure
EEPROM	BBCV (SIM)	128 kbyte	Instrument specific information: • Product identification (e.g. Serial number) • Product options • Operation time • Power-on count	no	None required (no user data)
EEPROM	FrontCV	2 kbit	Display infomation data	no	
Flash	BBCV	1 Gbit	Module-specific data: • FPGA startup file • Board data (e.g. MAC addresses for FPGA)	no	
Flash	BBCV (µController)	256 kbyte	Module-specific data: • MicroController program code • Board identification data	no	
Flash	RFCV (µController, storage component)	128 Mbit	Module-specific data: • MicroController program code • Board identification data • Board calibration data	no	
Flash	FrontCV (µController)	64 kbyte	Module-specific data: • MicroController program code • Board identification data • Backup for EDID data	no	

4.3 Media

Media are considered as non-volatile memory devices, as described in "Media" on page 6.

Table 4-3: Types of media memory modules

Memory type	Location	Size	Content	User data	Sanitization procedure
mSATA SSD	IPS3	64 Gbyte	• Operating system • Instrument firmware • Instrument internal correction data • Instrument states, e.g. Considerations for LAN Ports and setups • User data	Yes	see "Sanitize internal memory" on page 10

5 Instrument Declassification

Before you can remove the R&S SMCV100B from a secured area (for example to perform service or calibration), all classified user data needs to be removed. You can declassify the R&S SMCV100B as follows.

Remove power

1. Turn off the R&S SMCV100B.
2. Disconnect the power plug.

   Provided the instrument remains without power for at least five minutes, all volatile memory modules lose their contents, see [1].

Sanitize non-volatile memory

To sanitize the non-volatile memory media (mSATA SSD) depends on the setting of the volatile mode, provided by the instrument:

- If the volatile mode is disabled (default setting on the instrument):
  The R&S SMCV100B saves user data and instrument setups permanently on the mSATA SSD.
  Sanitization procedure: Sanitize internal memory procedure.
- If the volatile mode is enabled:
  The R&S SMCV100B redirects user data and instrument setups to the volatile memory.
  Sanitization procedure: Turn off instrument power.

Following these steps removes all user data from the R&S SMCV100B. The instrument can now leave the secured area.

Find more about setting the volatile mode in sections "Protecting Data" and "Disk & Memory Security Settings" of the user manual www.rohde-schwarz.com/manual/smcv100b.

Validity of instrument calibration after declassification

The EEPROM is the only memory type used to hold permanent adjustment values required to maintain the validity of the R&S SMCV100B's calibration. Therefore, the sanitizing procedure does not affect the validity of the instrument’s calibration.

5.1 Sanitization

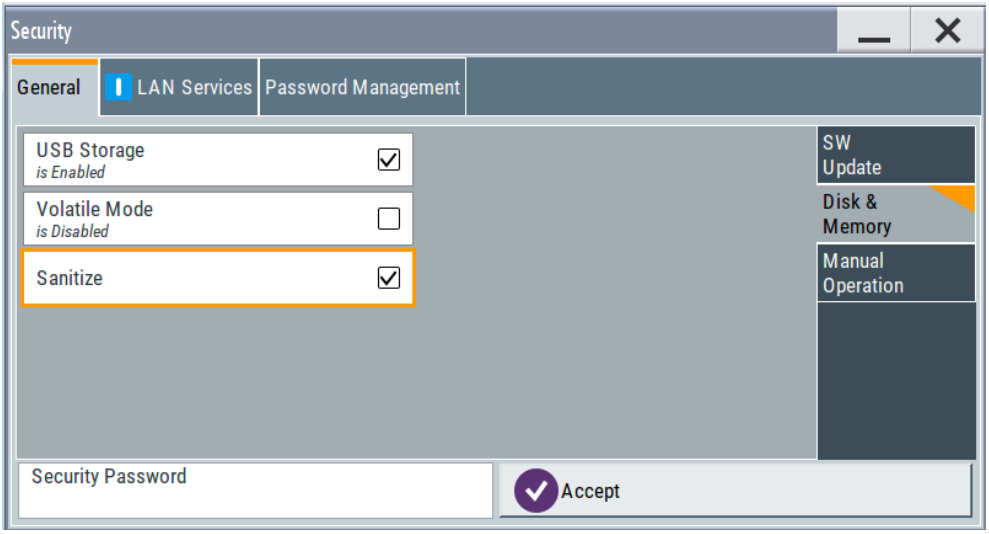
The mSATA SSD does not lose its contents when power is removed. It can contain user data.

Sanitize internal memory

You can clear the mSATA SSD by executing the sanitizing procedure provided on the instrument. The sanitizing procedure complies to the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 5.

Access:

1. Select "System Config > Setup > Security > General".
2. Select "Disk & Memory".



3. Enable "Sanitize".
4. Enter the "Security Password".
5. Confirm with "Accept".
6. **NOTICE!** Risk of instrument damage when interrupting the sanitizing procedure. Do not turn off or disconnect the R&S SMCV100B from the mains while the sanitizing procedure is running.

   The sanitizing procedure takes approximately 30 minutes.
   Wait until the instrument confirms the completed sanitizing.

6 Special Security Features

This section leads you to the information on how to use the security features to protect the R&S SMCV100B from unauthorized access of classified information saved or displayed in the instrument.

The user manual is provided for download on the product page at www.rohde-schwarz.com/manual/smcv100b.

6.1 Considerations for USB Interfaces

USB ports can pose a security risk in high-security locations. Generally, this risk comes from small USB pen drives, also known as memory sticks or key drives. They can be easily concealed and can quickly read/write several Gbyte of data.

See Recommended Security Settings > Chapter 7.1, "USB Interfaces", on page 12.

6.2 Considerations for LAN Interface

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

The R&S SMCV100B enables you, to disable the LAN interface and individually enable or disable the supported LAN interface services.

See Recommended Security Settings > Chapter 7.2, "LAN Interface and Services", on page 13.

6.3 Considerations for the User Interface

To prevent unauthorized personnel from reading the display during operation, you can disable the user interface, e.g. when you remotely control the instrument from a different location. You can lock only the status bar in the display, the entire screen and also the control elements on the front panel.

See Recommended Security Settings > Chapter 7.3, "Graphical User Interface (GUI)", on page 14.

7 Recommended Security Settings

Basically, see the user manual, chapter "General Instrument Functions > Using the Security Settings" for the security concept of the R&S SMCV100B, 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/smcv100b.

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.

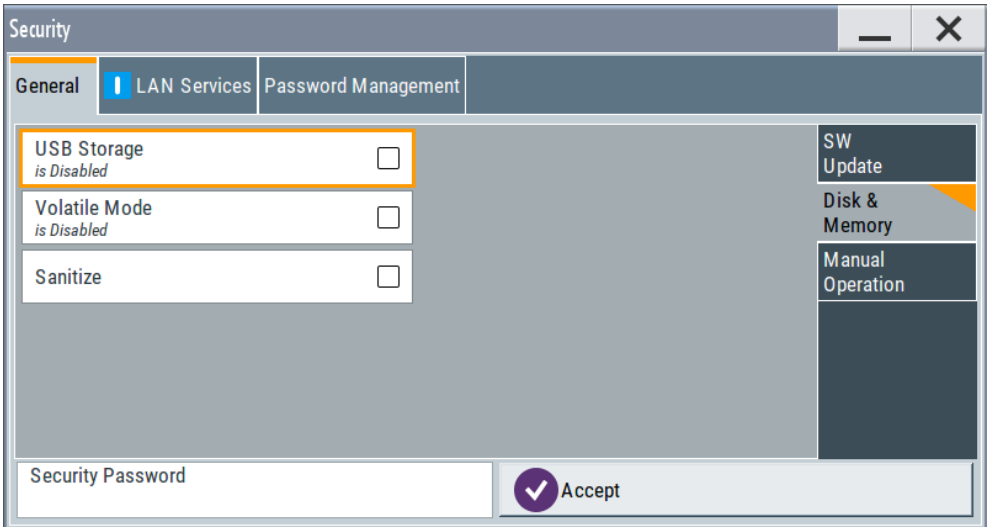
7.1 USB Interfaces

There are special considerations for R&S SMCV100B USB ports to avoid unauthorized data access in a high-security location.

Disabling USB ports for writing user data

To disable the write capability on the USB ports of the R&S SMCV100B:

1. Select "System Config > Setup > Security > General".
2. Select "Disk & Memory".
3. Disable "USB Storage".
4. Enter the "Security Password".
5. Confirm with "Accept".



When disabled, the R&S SMCV100B does not accept any USB memory device. After reboot, it also disables the USB write capability.

The setting does not affect USB devices without memory, such as a connected mouse or keyboard.

Remove all USB memory devices before disabling the USB storage. If any USB memory device remains connected, disabling is blocked, and the instrument returns a warning message.

7.2 LAN Interface and Services

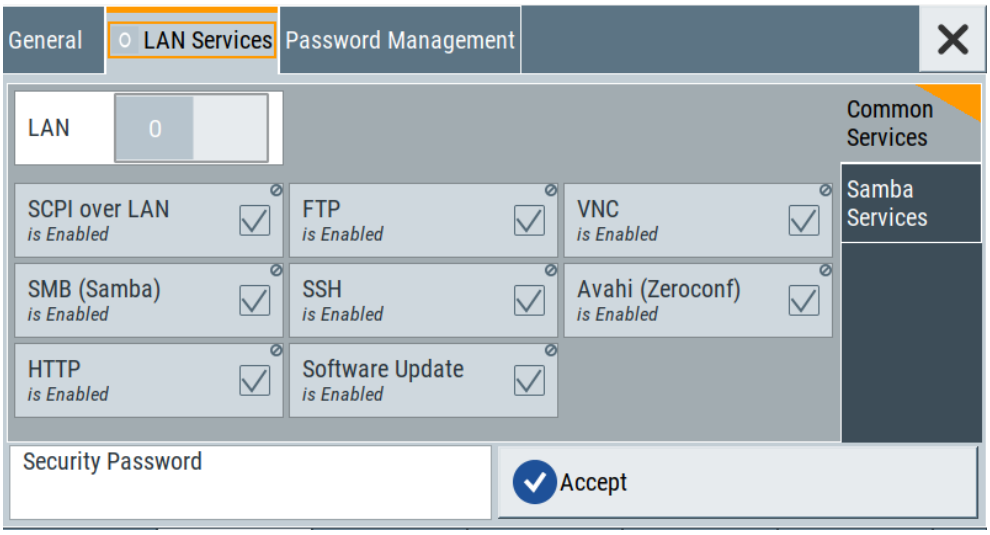
To protect the instrument against unauthorized data access in a high-security location, you can disable the LAN interface or individually enable or disable the supported LAN interface services.

We recommend that you disable all unused LAN ports and services.

Disabling LAN ports and services

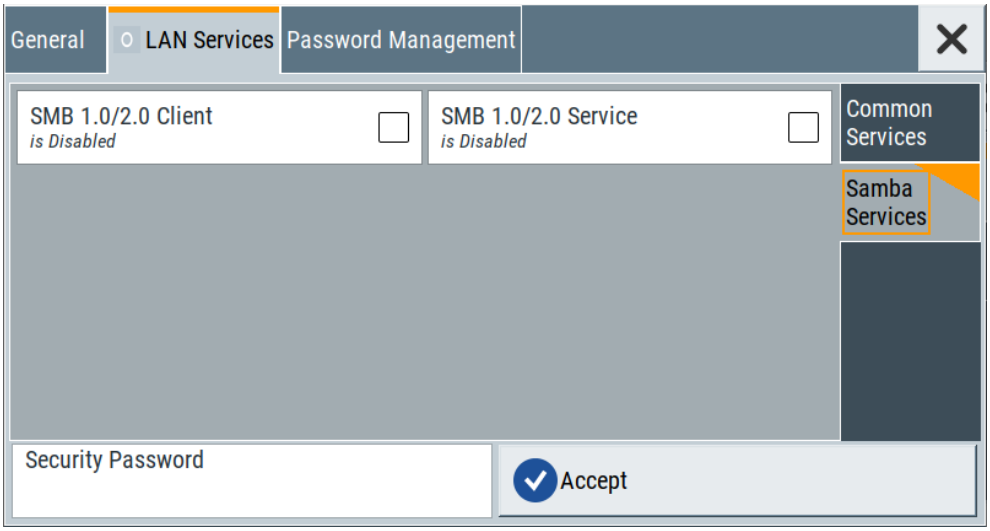
To disable the LAN ports and services of the R&S SMCV100B:

1. Select "System Config > Setup > Security > LAN Services".
2. In the "Common Services" side tab, disable the "LAN Interface".



You can also enable or disable LAN services individually, e.g. select "FTP > Off" or "VNC > Off".

3. Select the "Samba Services" side tab.



In this tab, you can enable or disable predecessor versions of the SMB client and SMB server.

4. Enter the "Security Password".
5. Confirm with "Accept"

   When disabled, it is not possible to establish a LAN connection to the R&S SMCV100B, or over the individually disabled services.

7.3 Graphical User Interface (GUI)

To protect the instrument against unauthorized personnel from reading the display, you can lock the display and the front panel controls.

Disabling the frequency and level indication in the status bar

These settings are useful to prevent unauthorized personnel from reading the display, when you remotely control the instrument from a different location.

1. Select "System Config > Setup > Security > General > Manual Operation".
2. Select "Annotation Frequency > Off" or "Annotation Amplitude > Off".
3. Enter the "Security Password".
4. Confirm with "Accept"

Deactivating the user interface

To lock the user interface:

1. Select "System Config > Setup > Security > General > Manual Operation".
2. Select "User Interface > Disabled".
   Locks the display and all controls for manual operation.

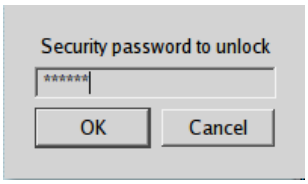
As an alternative, you can lock the display and controls individually with the following settings:
Select "User Interface" > ...

UI selection	Locked	Still enabled	Unlockable with:
"Touchscreen Off"	Touchscreen functionality Displays the touchscreen locked icon .	Front panel controls External controls VNC remote operation	External controls VNC remote operation Remote control
"VNC only"	Front panel controls External controls Displays the VNC icon .	VNC remote operation Screen display	VNC remote operation Turn off and on again.
"Display only"	Touchscreen functionality Front panel controls External controls Displays a padlock icon .	Screen display	Security password.
"Disabled"	Display Touchscreen functionality Front panel controls External controls Displays a padlock icon .	Remote control	Security password.

3. Enter the "Security Password".
4. Confirm with "Accept".

Unlocking the user interface for manual operation

1. In manual operation:
   a) On the instrument's keypad or external keyboard, press any key.
   The instrument prompts you to enter the security password for unlocking.



   Note: The R&S SMCV100B immediately inserts the character of the first key you pressed into the input field.
   b) Delete the entry before inserting the password.
   Enter the security password.
2. In remote control mode:
   a) Send the command `SYST:ULOC ENABled` to release all locks at once.
   b) Send the command `SYST:KLOC OFF` to unlock the keyboard and touchscreen.
   c) Send the command `SYST:DLOC OFF` to release all locks.

   Via remote control, there is no password required.

Glossary: Terminology for Instrument Security Procedures

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