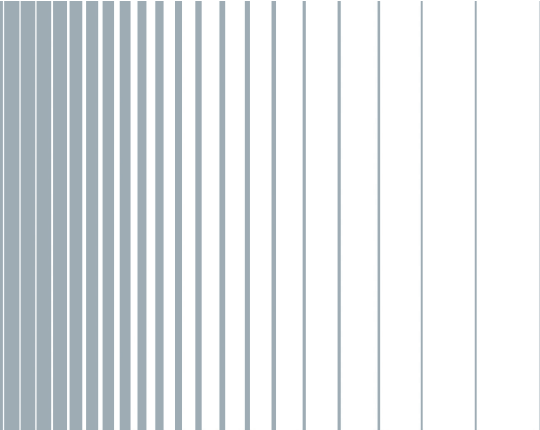


R&S®SMB100B

RF Signal Generator

Instrument Security Procedures



1 Overview

In many cases, it is imperative that the R&S SMB100B RF signal generators are used in a secured environment. Generally these 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. Security concerns can arise when devices need to leave a secured area e.g. to be calibrated or serviced.

This document describes the types of memory and their usage in the R&S SMB100B. It provides a statement regarding the volatility of all memory types and specifies the steps required to declassify an instrument through memory clearing or sanitization procedures. These sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS).

2 Instrument Models Covered

Table 2-1: RF signal generator models

Product name	Order number
R&S SMB100B	1422.1000K02

3 Security Terms and Definitions

Clearing

The term "clearing" is defined in Section 8-301a of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)". Clearing is the process of eradicating the data on media so that the data can no longer be retrieved using the standard interfaces on the instrument. Therefore, clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.

Sanitization

The term "sanitization" is defined in Section 8-301b of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)". Sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned for service of calibration.

The memory sanitization procedures described in this document are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are specified in the "Clearing and Sanitization Matrix" in Section 14.1.16 of the ISFO "Manual for the Certification and Accreditation of Classified Systems under the NISPOM".

Instrument declassification

The term "instrument declassification" refers to procedures that must be undertaken before an instrument can be removed from a secure environment, for example when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. The declassification procedures described in this document are designed to meet the requirements specified in DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", Chapter 8.

4 Types of Memory and Information Storage in the R&S SMB100B

The RF signal generator contains various memory components.

The following table provides an overview of the memory components that are part of your instrument. For a detailed description regarding type, size, usage and location, refer to the subsequent sections.

Table 4-1: Types of memory and information storage

Memory type	Size	Content	Volatility	User data	Sanitization procedure
SDRAM (CPU board)	1 GByte	Temporary information storage for operating system and instrument firmware, or RAM disk for user data	Volatile	Yes	Turn off instrument power
EEPROM/Flash (one per module)	256 Byte up to 4 MByte	Module-specific data: <ul style="list-style-type: none"> Serial number Board internal correction data 	Non-volatile	No	None required (no user data)
Flash (CPU board)	8 MByte	BIOS	Non-volatile	No	None required (no user data)
microSD memory card (CPU board)	1 GByte	<ul style="list-style-type: none"> Instrument states, e.g. USB port, LAN services and setups Instrument internal correction data User data 	Non-volatile	Yes	see " Sanitize internal memory " on page 5

4.1 Volatile Memory

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.

Removing power from this memory meets the memory sanitization requirements specified in the Clearing and Sanitization Matrix in section 5.2.5.5.5 of the ISFO Process

Manual for the Certification and Accreditation of Classified Systems under the NIS-POM.

SDRAM

The SDRAM on the CPU board contains temporary information storage for operating system and instrument firmware. The SDRAM loses its memory when power is removed.

Sanitization procedure: Turn off instrument power.

4.2 Non-Volatile Memory

The R&S SMB100B contains no user-accessible non-volatile memory, except for the microSD memory card on the CPU board. The microSD memory card on the CPU board can require a sanitization procedure, depending on specific conditions, see [microSD memory card \(CPU board\)](#).

All other non-volatile memories of the R&S SMB100B are not a security concern.

EEPROM/Flash (module memory)

Every module, except the CPU board, is equipped with a persistent module memory, which can be EEPROM or Flash memory. These module memories contain module-specific data, such as the serial number of the module and correction data. The EEPROM does not hold user data nor can the user access the EEPROM storage.

Sanitization procedure: None required (no user data).

Flash (CPU board)

The flash memory contains the BIOS. It is on the CPU board of the R&S SMB100B. This flash memory does not hold user data nor can the user access the flash memory.

Sanitization procedure: None required (no user data).

microSD memory card (CPU board)

The R&S SMB100B saves user and application data on the microSD memory card permanently, provided the **volatile mode** on the instrument is **disabled** (default setting).

If the volatile mode is enabled, no user data can be written to the internal memory permanently. 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/smb100b.

The microSD memory card holds the data and is non-volatile. Hence, data is not erased when power is removed from the instrument.

Sanitization procedure: [Sanitize internal memory](#) procedure.

5 Secure Erase Procedures

Because the volatile memory types are erased when power is removed from the RF signal generator, they do not pose a security risk. The flash memories on the CPU board contain no user data. Therefore, it is deemed that they do not pose a risk either.

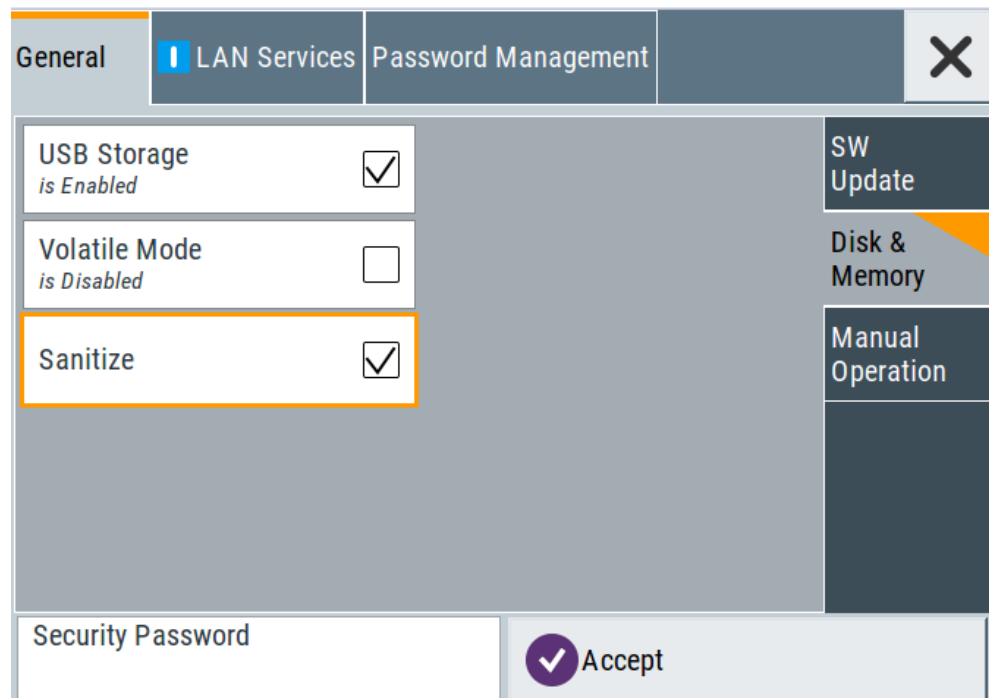
The microSD memory card on the CPU board does not lose its contents when power is removed. It can contain user data.

Sanitize internal memory

You can sanitize the microSD memory card on the CPU board flash memory by executing the sanitizing procedure provided on the instrument:

Access:

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



3. Enable "Sanitize".
4. Enter the "Security Password".
5. Confirm with "Accept".

Note: The default password is 123456. For more information, see section "Using the Security Settings" in the R&S SMB100B user manual (see www.rohde-schwarz.com/manual/smb100b).

The Secure Erase Procedure meets the memory sanitization requirements specified in the Clearing and Sanitization Matrix in section 14.1.16 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.

6 Instrument Declassification

Before you can remove the RF signal generator from a secured area, e.g. to perform service or calibration, all classified user data needs to be removed.

You can declassify the R&S SMB100B as follows:

- ▶ Execute the sanitization procedure, as described in [Sanitize internal memory](#) procedure.

Following these steps removes all user data from the RF signal generator.

The R&S SMB100B can now leave the secured area.

These declassification procedures meet the needs of customers working in secured areas.

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 SMB100B's calibration.

7 Special Considerations for USB Ports and LAN Services

There are special considerations for R&S SMB100B USB ports and LAN services to avoid unauthorized data access in a high-security location.

The access states of the USB ports and LAN services are saved according to [Table 4-1](#).

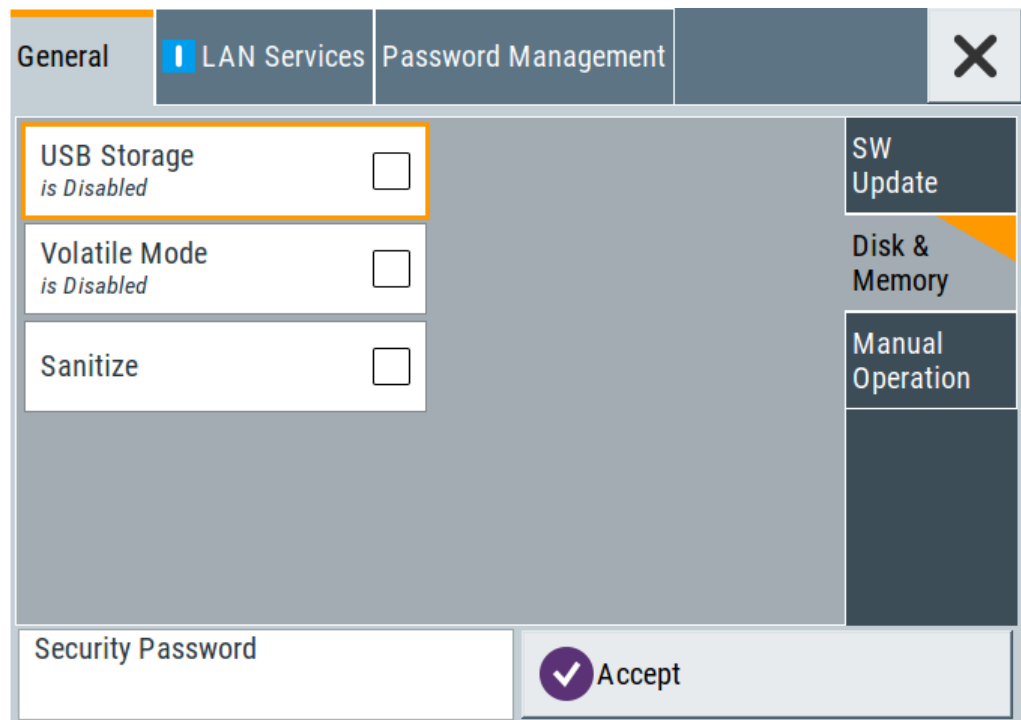
7.1 Special Considerations for USB Ports

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. To protect the instrument against unauthorized data access, you can disable the USB interface.

Disabling USB ports for writing user data

To disable the write capability on the USB ports of the R&S SMB100B:

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, no USB storage device is accepted by the instrument. After a reboot of the instrument, the write capability on any USB memory device is disabled. Other non-memory USB devices (such as keyboards and mice) are not affected.

7.2 Special Considerations for LAN Ports

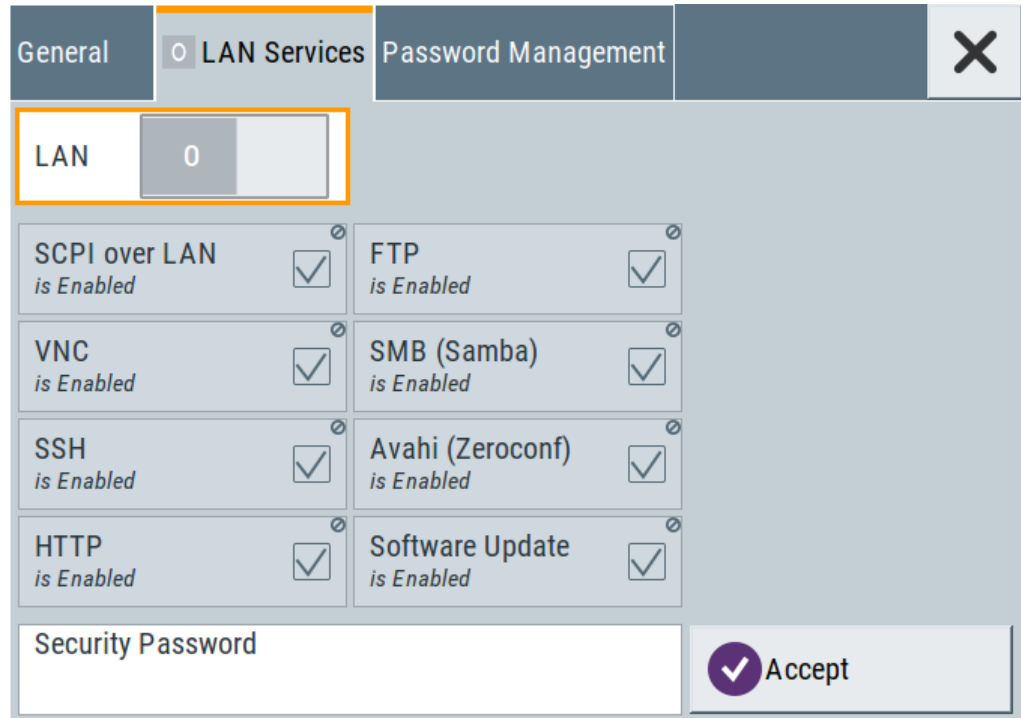
To protect the instrument against unauthorized data access in a high-security location, you can disable the LAN interface.

Disabling LAN ports

To disable the LAN ports of the R&S SMB100B:

1. Select "System Config > Setup > Security > LAN Services".

2. Disable the "LAN" interface.
3. Enter the "Security Password".
4. Confirm with "Accept"



When disabled, no LAN connection can be established with the instrument.

For information concerning the security features, refer also to the R&S SMB100B user manual.

© 2018 Rohde & Schwarz GmbH & Co. KG
 Mühldorfstr. 15, 81671 München, Germany
 Phone: +49 89 41 29 - 0
 Fax: +49 89 41 29 12 164
 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.

Throughout this manual, products from Rohde & Schwarz are indicated without the ® symbol, e.g. R&S®SMB100B is indicated as R&S SMB100B.