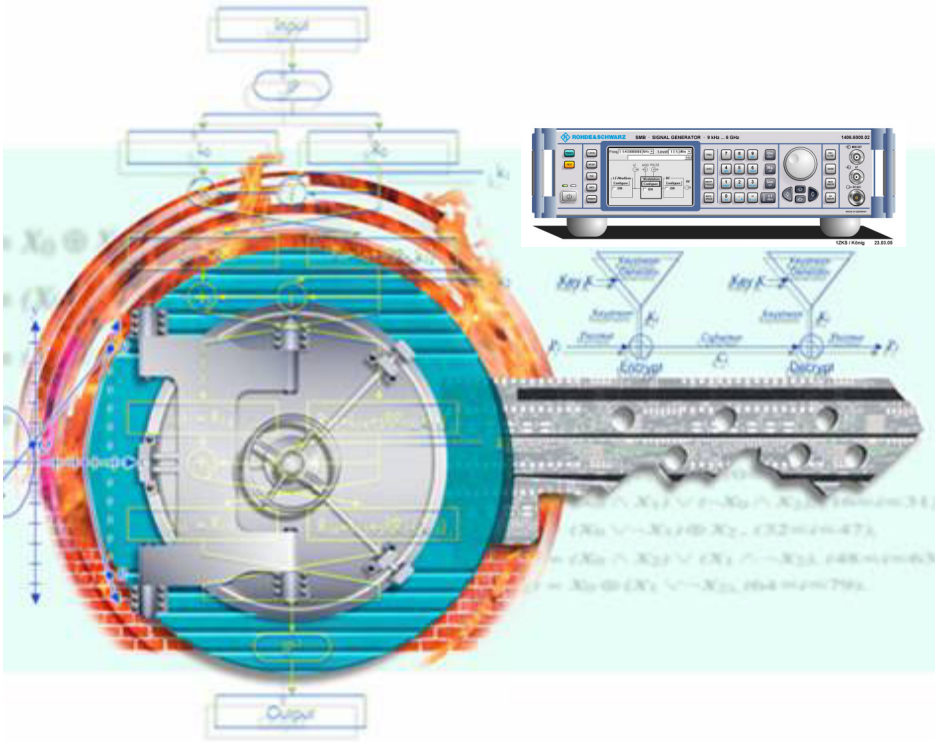

Product: Signal Generator R&S® SMB100A

Resolving Security Issues when working with the R&S® SMB100A in Secure Areas

Based upon the user's security requirements, this document describes the Rohde & Schwarz options available to address the user's signal generator needs. It also covers the different memory types and locations where user information can be stored in the signal generator R&S® SMB100A. This document does not cover other R&S® signal generators.

For secure environments, it describes an approach to irretrievably remove user data and any information regarding instrument usage from the signal generator.

ROHDE&SCHWARZ

Overview

In many cases it is imperative that the R&S® SMB100A signal generator can be used in a secured environment. Generally these highly secured environments will not allow any test equipment to leave the area unless it can be proven that no user information will leave with the test equipment. Security concerns can arise when signal generators need to leave a secured area to be calibrated or serviced.

In the following the types of memory and their usage in the R&S® SMB100A signal generator is described. It also addresses methods of ensuring that no user data will leave the secured area if the product has to be removed for calibration or service needs.

The operating system of the R&S® SMB100A is LINUX.

Instrument Models Covered

R&S Signal Generator

R&S® SMB100A

Types of Memory in the R&S® SMB100A and its Security Concerns

SDRAM Memory

The R&S® SMB100A is equipped with 256 Mbyte[1] of SDRAM memory on the CPU board. SDRAMs are volatile memories. This kind of memory requires continuing power supply and data refresh to maintain data. Hence SDRAM loses data several minutes after power supply is switched off.

The SDRAM is not a security concern.

CMOS-RAM Memory

The R&S® SMB100A contains a real-time clock powered by an internal lithium battery. This battery is the only one used on the R&S® SMB100A and it is located on the CPU board. Unlike real-time clocks known from PCs, the R&S® SMB100A clock chipset does not contain CMOS-RAM memory.

The CMOS-RAM is not a security concern.

EEPROM Memory

The RF module al well as the processor module are equipped with in total four serial EEPROMs. These EEPROMs provide a capacity from 4 Kbyte[1] to 1 Mbyte[1] and contain module-relevant data such as initial processor configuration data, serial number of modules, calibration data etc. In addition, the current setting of the Standby-Button is saved here in order to restart instrument properly in case of power loss. The EEPROMs cannot be accessed by the user and they are not modified during instrument operation. Data will be changed by service centers when the R&S® SMB100A or the modules are calibrated.

The EEPROM memories are not a security concern.

Smartcard Memory

The processor module is equipped with a smartcard containing 32 KByte[1] of memory. It contains instrument specific data like serial number, personality and assembly. In addition the counters for operating time and power on cycles may be stored here. The smartcard is initialized during production and later is modified only when instrument assembly changes or to maintain the counters. Data can not be accessed by the user. Beyond operating time it does not provide conclusions about instrument usage.

The smartcard memory is not a security concern.

[1] Memory size might be subject to changes without further notice

FLASH Memory

The main nonvolatile storage medium of the R&S® SMB100A is implemented by a single-chip FLASH memory, located on the processor board and providing 256 Mbyte[1] of storage. This memory contains boot code, maintenance and recovery system, the operating system and instrument firmware. **Furthermore user data, instrument and password settings are stored here.**

The FLASH memory is logically divided into three sections:

<table>
<tr><td rowspan="2">Boot code
OS Kernel
8 MByte</td><td rowspan="2">Recovery
Area
64 MByte</td><td colspan="3">JFFS File System (security concern, sanitizable)</td></tr>
<tr><td>OS Files</td><td>Firmware</td><td>User Data, Instrument Settings</td></tr>
</table>

The first 8 MByte[1] contain boot code and the operating system kernel. This area is initialized during production and may be updated in case of firmware update. It cannot be accessed by the user and is not modified during instrument operation.

The next 64 MByte[1] contain recovery data which is used to restore the factory instrument configuration if required. This area is initialized during production. It cannot be accessed by the user and is not modified during instrument operation.

The remaining memory is controlled by a JFFS file system (Journaling Flash File System). This area is shared between operating system files, instrument firmware and user data. Operating system files and instrument firmware are encapsulated in preconfigured, read-only squashfs file systems. Both can not be modified during instrument operation nor can they be modified in parts. During firmware update they will be replaced in total.

In the remaining JFFS area the following information is stored:

- User data
- Passwords (see Chapter “Passwords Types”)
- LAN and USB port enable/disable states
- Internal Adjustment data

The JFFS area of the FLASH memory may be a security concern.

To meet security requirements, the whole JFFS area is sanitizable, as described later.

[1] Memory size might be subject to changes without further notice

Information Storage in the R&S® SMB100A Signal Generator

DATA	**SDRAM memory** Not a security concern	**EEPROM memory** Not a security concern	**Smartcard memory** Not a security concern	**FLASH memory** Potential security concern
Temporary information storage for the CPU (CPU, Cache and Swap Area)	N			
Hardware Information Instrument Serial Number Product Options Operation Time Power On Count			N	
Calibration and correction constants Module specific data like serial number, revision and options		N		
Initial CPU configuration data		N		N
Internal Adjustment data				N
Operating System and Instrument Firmware				N
Instrument states and setups, e.g. user frequencies and levels				S
User data and derived files, e.g. List Mode data				S

N = No security concern

S = Security concern

Information Security in Highly Sensitive Areas

Since the SDRAM is erased when power is removed from the signal generators, it does not pose a security risk. No user data is written to the EEPROM and smartcard memories; hence, it is deemed that they do not pose a risk either.

The internal FLASH memory is the only device that does not lose its contents when power is removed and may contain user data as well as confidential instrument configuration in its JFFS area.

To meet security requirements, the R&S® SMB100A provides a sanitizing procedure that ensures that user data will be irretrievably extinguished without removing storage from the instrument. The sanitizing procedure is part of the R&S® SMBs maintenance system which can be accessed by pressing and holding the rotary knob immediately after power on.

After activating the sanitizing procedure, the following steps occur:

- The file **rootfs.squashfs** (read-only, encapsulating operating system files) and the file **optfs** (read-only, encapsulating instrument firmware) are temporarily saved in SDRAM.
- A full sector erase command as per manufacturer data sheet is applied to every single sector of the JFFS area. This explicitly includes sectors which might be declared as defect.
- Every addressable location of the JFFS area is overwritten by a single character.
- Again, a full sector erase command as per manufacturer data sheet is applied to every single sector of the JFFS area, including defect sectors.
- The JFFS file system is recreated and operating system files as well as instrument firmware are restored.

This procedure meets the following requirements:

- **It is according to DOD 5220.22-M [NISPOM 8-306]**
- User data, passwords and other confidential data will be irretrievably destroyed.
- This also applies to data fragments stored in deleted files or in memory blocks marked as defective during instrument operation.
- Passwords are reset to factory values, USB and Ethernet interfaces are enabled.
- After sanitizing the instrument is operational. Firmware version is not affected.

Performing Service, Calibration and Maintenance on the R&S® SMB100A

The instrument calibration ensures that measurements are traceable to government standards. Rohde & Schwarz highly recommends that users follow the calibration cycle suggested for their instrument.

To hold classified user data in the secure areas while instrument is in service, Rohde & Schwarz recommends sanitizing the internal FLASH memory.

- Turn-off the signal generator. Press rotary knob and hold it while switching on instrument again. After a few seconds the screen of the maintenance system appears.

- Now you have the option to save the instrument configuration including firmware and user data (but without passwords) to a USB mass memory, e.g. a memory stick. To perform this operation it is recommended to plug a USB hub together with a USB keyboard to the instrument. Connect the USB memory to the hub too, then perform "Backup internal memory to USB" and follow instructions. To protect user data this operation requires knowledge of the security password (refer to section "Password types"). Wait until operation completes, remove USB memory and keep it in the secure area.

- Now sanitize the internal memory by means of **"Sanitize internal memory"** and wait until operation completes. Afterwards power can be removed or instrument can be rebooted. During first reboot after sanitizing the internal adjustments are performed.

  Since permanent adjustment values are located in the instrument's EEPROMs the validity of the signal generator's calibration is maintained throughout the sanitization.

- **It is now save to move the instrument out of the secure area.**

- After service you have the option to restore instrument configuration. Power on instrument and wait until is operational. Plug in the memory stick containing the instrument configuration and follow instructions. The procedure is exactly the same as a firmware update. Note that instrument passwords are not restored by this procedure and must be set separately.

The sanitization procedure is also performed when activating "Factory Recover" and "Install firmware package" operations throughout the maintenance system.

Performing Firmware Updates in Sensitive Areas

Rohde & Schwarz highly recommends, but does not require, to maintain their instruments with the latest firmware updates. Firmware updates are encapsulated in update packages and are available from the R&S website. They safely can be transferred to the secure area by means of a USB storage, e.g. a memory stick. The R&S® SMB100A signal generators are equipped with USB ports as standard equipment and firmware updates are applied by this interface.

There are two options to safely perform this operation:

Firmware update via USB port while instrument is operating

When instrument is operating, firmware updates are initiated by connecting a USB storage containing an update package to the R&S® SMB100A.

This kind of firmware update does not modify user data nor does it change any of the passwords, LAN settings or LAN or USB port enable/disable states. It requires that the USB port has not been disabled in security settings, as described later. If so, the port must be re-enabled first.

Firmware update via USB port using the maintenance system

Powering on the R&S® SMB100A while holding the rotary knob pressed will enter the instruments maintenance system (firmware version 2.05 or higher). Firmware update can be initiated by performing the function "Install firmware package". This procedure does **not** require that the USB port is enabled.

Caution: This procedure sanitizes instruments FLASH memory before applying the update. User data and instrument settings are irretrievably lost, Password, LAN and USB settings are reset to factory values.

Password types

There are two different types of passwords available in the R&S® SMB100A:

- Security Password
- VNC Password

Both passwords will be reset to factory values by performing the sanitizing procedure.

Security Password

The security password protects the enabling/disabling states of LAN and USB storage.

Predefined password: 123456

In security sensitive areas it is recommended to change this password.

VNC Password

The VNC password protects access to the instrument via the remote control software VNC.

Predefined password: instrument

Caution: If the instrument is connected to a network it can be remote controlled by anyone who has knowledge of this password. Therefore it is recommended to change the password.

Special considerations for USB ports

USB ports can pose a security threat in high-security locations. Generally, this threat comes from small USB pen drives (also known as memory sticks, key drives, etc.) which can be very easily concealed, yet can quickly read/write several GBytes of data.

To disable USB Ports

The R&S® SMB100A signal generator can disable its USB port by means of firmware (Version 2.04 or higher): In the Setup/Security menu one can activate and deactivate the possibility to connect a USB mass storage device. To do so, the security password is required. The security password can be changed in the same dialog. It is recommended to actually change this password from its default. While deactivated no USB storage device will be accepted by the instrument. Other non-memory USB devices (such as keyboards, mice etc.) are not affected.

The enable/disable state of the USB port is stored on the instruments FLASH memory.

Special considerations for LAN ports

Some users select not to install a LAN within their high-security locations.

To disable LAN Ports

The R&S® SMB100A signal generator can disable its LAN ports by means of firmware (Version 2.04 or higher). In the Setup/Security menu one can activate and deactivate the LAN connector. To do so, the security password is required. The security password can be changed in the same dialog. It is recommended to actually change this password from its default. When deactivated no LAN connection can be established with the instrument.

The enable/disable state of the LAN port is stored on the instruments FLASH memory.

Additional Information

Please contact your support center for comments and further suggestions:

Support Center Europe

Telephone: +49 180 512 4242
Fax: +49 89 4129 63778
Internet: CustomerSupport@Rohde-Schwarz.com

Support Center America

Telephone: 1-888-TESTRSA (1-888-837-8772) selection 2
From outside the USA: +1-410-910-7988
Email: customer.support@rsa.rohde-schwarz.com

Support Center Asia

Telephone: +65 6 513 0488
Fax: +65 6 8461060
E-mail: customersupport.asia@rohde-schwarz.com

ROHDE & SCHWARZ GmbH & Co. KG · Mühldorfstraße 15 · D-81671 München ·
P.O.B 80 14 69 · D-81614 München · Telephone +49 89 4129 -0 · Fax +49 89 4129 - 13777 ·
Internet: http://www.rohde-schwarz.com