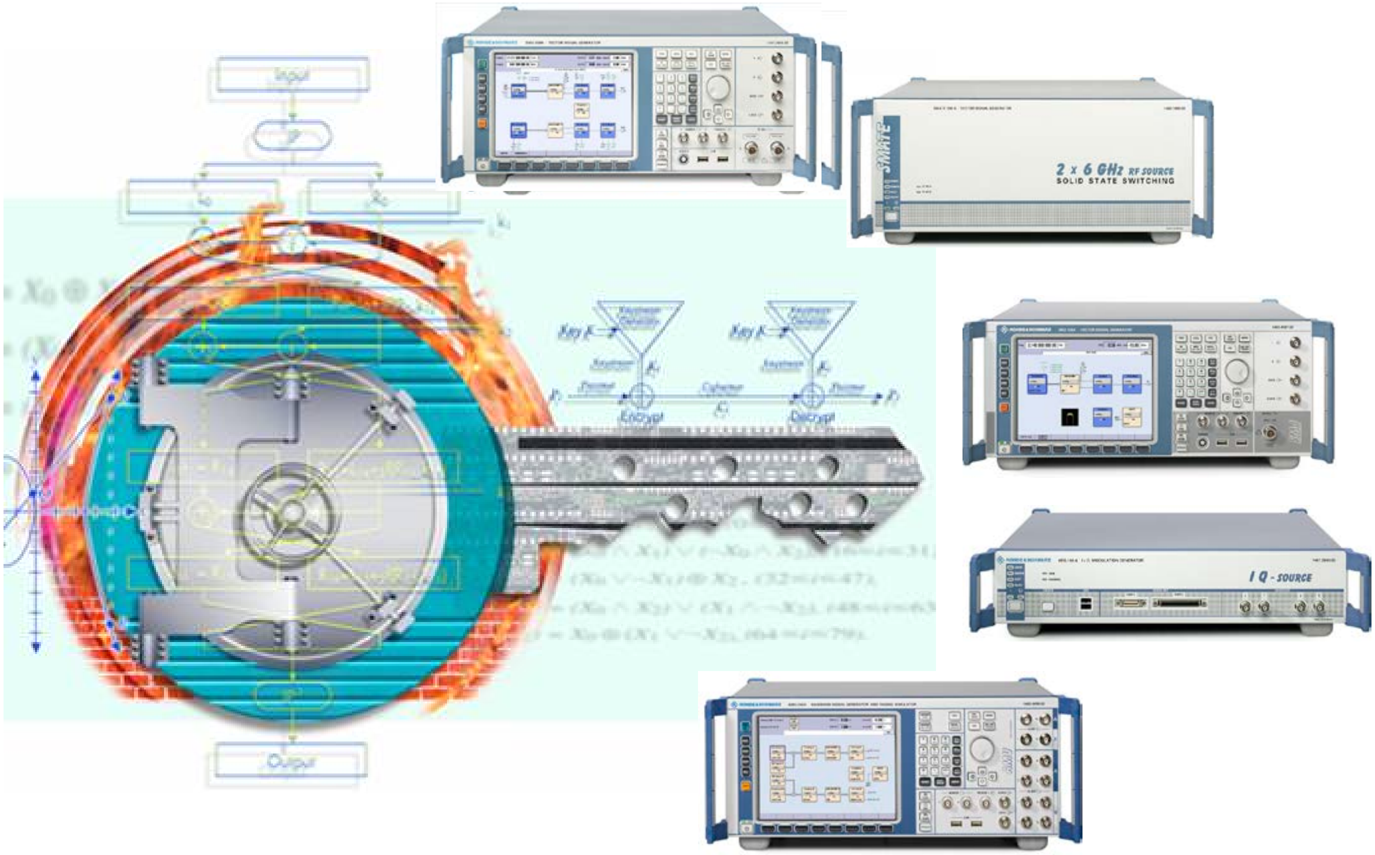

Products: Signal Generators

R&S® SMU200A, R&S® SMATE200A, R&S® SMJ100A, R&S® AMU200A, R&S® AFQ100A

Resolving Security Issues when working with R&S® SMU200A, R&S® SMATE200A, R&S® SMJ100A, R&S® AMU200A, or R&S® AFQ100A 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® SMU200A. In addition this document also covers the following R&S® Signal Generators :

R&S® SMATE200A, R&S® SMJ100A, R&S® AMU200A and R&S® AFQ100A

ROHDE&SCHWARZ

Overview

In many cases it is imperative that R&S® SMU200A, R&S® SMATE200A, R&S® SMJ100A, R&S® AMU200A or R&S® AFQ100A 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® SMU200A, R&S® SMATE200A, R&S® SMJ100A, R&S® AMU200A or R&S® AFQ100A signal generators 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.

Instrument Models Covered

R&S Signal Generator

R&S® SMU200A

R&S® SMJ100A

R&S® SMATE200A

R&S® AMU200A

R&S® AFQ100A

In the following document, as instrument it is always referred to the R&S® SMU200A while the information is valid for all models covered. If there are some special points for one specific instrument, it is given and stated clearly.

Battery Information

The only battery used on the R&S® SMU200A is located on the CPU board. This battery is used exclusively for powering the real-time clock in the chipset and the CMOS-SRAM memory. The CMOS-SRAM memory is used only to store the BIOS setup.

The CMOS-SRAM is not a security concern.

Types of Memory in the R&S® SMU200A and its Security Concerns

SDRAM Memory

The R&S® SMU200A has 256/512 Mbyte of SDRAM memory on the CPU board. SDRAMs are volatile memories and lose their data when the power supply is switched off. The SDRAM will be unreadable within one minute after the power is removed from the instrument.

The SDRAM is not a security concern.

EEPROM Memory

Every module, with the exception of the motherboard, is equipped with a serial EEPROM. These EEPROMs have a capacity of 2 Kbyte (memory size might be subject to changes without further notice) and contain module-relevant data such as the serial number of the module, calibration data, etc., and cannot be accessed by the user. The data can only be changed by the service center when the R&S® SMU200A or the module is calibrated. User data cannot be stored on the EEPROM memory

The EEPROM is not a security concern.

FLASH Memory

There are two FLASH memories in the R&S® SMU200A. The first 512k FLASH memory contains the BIOS. It is on the CPU board of the R&S® SMU200A.

The second 1 Mbyte FLASH memory contains module-relevant data such as the serial number of the module, options, calibration data, etc. It is located on the motherboard of the R&S® SMU200A.

The user cannot access either memory. The FLASH memory data can only be changed by the service center when the R&S® SMU200A or the module is calibrated.

The FLASH memory is not a security concern.

Hard Drive

The hard drive is the nonvolatile storage medium in the R&S® SMU200, with the exception of the R&S® AFQ100 instruments, which are eqiupped with a removable hard disc (see *Removable Hard Disc of the R&S® AFQ100A*).

Because the hard drive is nonvolatile, user data is not erased when power is removed from the instrument.

The following information is stored on hard drive:

- The R&S® SMU200A 's operating system (Microsoft Windows®)
- The R&S® SMU200A's firmware
- Instruments states, setups and user data (e.g. waveforms)

The hard drive is a security concern.

Removable Hard Disc of the R&S® AFQ100A

The removable hard disc, 160 Gbyte is the nonvolatile storage medium in the R&S® AFQ100A. Because the hard disc is nonvolatile, user data is not erased when power is removed from the instrument.

The following information is stored on the hard disc:

- Instrument settings (manually saved instrument setups)
- User data (like waveforms or list mode data) and temporary files needed to create these files.

The removable hard disc allows a user to remove the hard disc from the signal generator. The hard disc can thus be removed from the R&S® AFQ100A before it leaves the high-security area.

The hard disc is not a security concern.

Information Storage in the R&S® SMU200A Signal Generator

DATA	SDRAM	FLASH	EEPROM	HARD DRIVE		R&S® AFQ100A Removable Hard Disc
Temporary Information storage for the CPU (CPU, Cache and Swap Area)	N			N		
Hardware Info, Serial Number, Product Options and Calibration Correction Constants Operation Time Power On Count Relays switching Count		N				
BIOS and Module Relevant Data such as the module serial number and options			N			
Operating System and Instrument Firmware				N		
Instruments states, setups and user data (e.g. waveforms)				S		N

N = No security concern

S = Security concern

Maintaining Security / Sanitizing

Clearing the different types of memory.

SDRAM

This memory is volatile. All you have to do is remove the power from the instrument and all data stored in it will be lost.

Hard Drive

All user specific data like

- Instrument states and setups
- Waveforms, data lists, list mode lists, …

is stored on the internal hard drive or for the R&S® AFQ100A instruments, on the removable hard disc, respectively. Simply deleting these files is not sufficient from a security perspective.

To meet security requirements, the R&S® SMU200A provides a sanitizing procedure that ensures that user data will be irretrievably extinguished without removing storage from the instrument.

Notice to R&S® AFQ100A

Do not use the function ***Initialize Hard Disc*** *for sanitizing. It is only intended for setting up the hard disc.*

All necessary parts and tools are available from the R&S service department:

- Recovery CD with sanitizing program
- External CD drive
- Spare hard disks (in case of the hard disk must be destroyed physically)

Sanitizing

To sanitize an R&S® SMU200A, perform the following steps:

1. Connect the external CD drive to the instrument
2. Insert the Recovery CD
3. Boot the instrument
4. Select “Wipe disk” from the menu

After sanitization the instrument is not operational. The following two steps must be performed in order to repair it:

1. Recover the operating system by using the Recovery CD
2. Install the firmware from USB. The newest version (recommended) can be downloaded from www.rohde-schwarz.com, older versions can be retrieved from the R&S service department.

This sanitization meets the following requirements:

1. **It is according to DOD 5220.22-M [NISPOM 8-306]**
2. User data, passwords and other confidential data will be irretrievably destroyed.
3. This also applies to data fragments stored in deleted files or in memory blocks marked as defective during instrument operation.
4. Passwords are reset to factory values, USB and Ethernet interfaces are enabled.

In the case hard disks must be destroyed physically, empty hard disks are also available from the R&S service department. The replacement is explained in detail in the service manual delivered with R&S® SMU200A.

Performing Firmware Updates and Backing-up User Data in Sensitive Areas

Rohde & Schwarz highly recommends, but does not require, the users of its products, to maintain their products with the latest updates and to regularly back-up important user data that can be erased. Firmware updates are available from the R&S website. How does a user perform firmware updates and back-up user data in sensitive areas? There are several options available for the user to safely perform these operations without compromising the security of the sensitive areas.

Via the USB port

R&S® SMU200A signal generators are equipped with USB ports as standard equipment. As described below, users can disable these ports. For users that have not elected to disable the USB ports a memory stick can be used to transport a firmware update into a secure area. The instrument firmware update can be performed directly from the USB stick. The USB stick can likewise hold or transport user data back-ups to an approved storage medium.

Via LAN

R&S® SMU200A signal generators are equipped with LAN as standard equipment. As described below, users can disable these ports. For users that have not elected to disable the LAN the LAN interface can be used to transport the firmware update onto the instrument. There the firmware update can be stored on the internal hard drive. From the hard drive the update can be performed.

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 (a.k.a. memory sticks, key drives, etc) which can be very easily concealed, yet can quickly read/write several GBytes of data.

To disable USB Ports

Firmware version below 2.04[1]

R&S® AFQ100A only:

The R&S® AFQ100A signal generator can disable its USB port by means of BIOS. Setting a BIOS password is recommended.

All other equipment need firmware version 2.04 at least to disable the USB ports.

Firmware version 2.04[1] or higher

The R&S® SMU200A (likewise the R&S® SMJ100A, R&S® SMATE200A) signal generator can disable its USB port by means of firmware (starting from December 2006): In the Setup/Security menu, one can activate and deactivate the possibility to connect a USB mass storage device. To do so, the root password is required. The root password can be changed in the same dialog. It is recommended to actually change this password from its default, see manual for details. When deactivated no USB mass storage device can be connected.

[1] Firmware version 2.04 will be available from December 2006.

Special considerations for LAN ports

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

To disable LAN Ports

Firmware version below 2.10

R&S® AFQ100A only:

The R&S® AFQ100A signal generator can disable its LAN ports by means of BIOS. Setting a BIOS password is recommended.

Firmware version 2.10 or higher

The R&S® SMU100A (likewise the R&S® SMJ100A, R&S® SMATE200A) signal generator can disable its LAN ports by means of firmware (starting from December 2006). In the Setup/Security menu, one can activate and deactivate the LAN connector. To do so, the root password is required. The root 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.

Additional Information

Please contact your Rohde & Schwarz support center for comments and further suggestions, or find the current address on the homepage http://www.customersupport.rohde-schwarz.com.

Regional contact:

Europe, Africa, Middle East
+49 1805 12 42 42* or
+49 89 4129 137 74
customersupport@rohde-schwarz.com

North America
1-888-TEST-RSA (1-888-837-8772)
customer.support@rsa.rohde-schwarz.com

Latin America
+1-410-910-7988
customersupport.la@rohde-schwarz.com

Asia/Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

ROHDE & SCHWARZ
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