Products: Signal Generators R&S® SMA100A and R&S® SMF100A

Resolving Security Issues
when working with the
R&S® SMA100A or R&S® SMF100A
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 generators R&S® SMA100A or R&S® SMF100A. This document does not cover other R&S® signal generators.

For secure environments, it describes an approach to physically remove the user data from the signal generator.
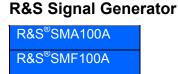
ROHDE & SCHWARZ

Overview

In many cases it is imperative that R&S® SMA100A or R&S® SMF100A signal generators 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® SMA100A or R&S® SMF100A 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.

The operating system of the R&S® SMA100A and the R&S® SMF100A is LINUX. LINUX is more robust in terms of security issues like viruses and security holes.

Instrument Models Covered

R&S Signal Generator

R&S®SMA100A
R&S®SMF100A

Types of Memory in the R&S® SMA100A / R&S® SMF100A and its Security Concerns

CMOS-RAM Memory

The CMOS-SRAM memory is used only to store the BIOS setup. The CMOS-RAM is powered by the internal battery (which also powers the real-time clock in the chipset). It is the only battery used on the R&S® SMA100A / R&S® SMF100A and is located on the CPU board.

The CMOS-RAM is not a security concern.

SDRAM Memory

The R&S® SMA100A / R&S® SMF100A has 256 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® SMA100A / R&S® SMF100A 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® SMA100A / R&S® SMF100A. The first 512 Kbyte FLASH memory contains the BIOS. It is on the CPU board of the R&S® SMA100A / R&S® SMF100A.

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® SMA100A / R&S® SMF100A.

The user cannot access either memory. The FLASH memory data can only be changed by the service center when the R&S® SMA100A / R&S® SMF100A or the module is calibrated.

The FLASH memory is not a security concern.

Removable and Non-removable CompactFlash™ Memory

The CompactFlash™ Memory card (256 Mbyte) is the nonvolatile storage medium in the R&S® SMA100A / R&S® SMF100A. Because the CompactFlash™ Memory card is nonvolatile, user data is not erased when power is removed from the instrument.

The following information is stored on the CompactFlash™ Memory card:

- The R&S® SMA100A's / R&S® SMF100A's operating system (LINUX)

- The R&S® SMA100A's / R&S® SMF100A's firmware

- User data

- Passwords (see Chapter "Types of used Passwords")

- LAN and USB port enable/disable states

The R&S® SMA100A / R&S® SMF100A has an option (the R&S® SMA-B80 / R&S® SMF-B85) that allows a user to remove the CompactFlash™ Memory card from the signal generator by means of a card ejector. The CompactFlash™ Memory card can thus be removed from the R&S® SMA100A / R&S® SMF100A before it leaves the high-security area.

The Removable and Non-removable CompactFlash™ Memory should be treated differently with respect to security concerns.

- ➢ **The Removable CompactFlash™ Memory (option R&S® SMA-B80 / R&S® SMF-B85) is not a security concern because it <u>can be removed</u> from the instrument and left in the secure area.**

- ➢ **The Non-removable CompactFlash™ Memory (i.e. an R&S® SMA100A without the option R&S® SMA-B80 / R&S® SMF100A without the option R&S® SMF-B85) can pose a security concern because it <u>cannot be removed</u> from the instrument.**

There is a Spare CompactFlash™ Memory card available (R&S® SMA-Z10 / R&S® SMF-Z10). This card includes the operating system and the instrument firmware. The card is not bound to a specific R&S® SMA100A / R&S® SMF100A. It can be interchanged between different units. Only the internal adjustments of the R&S® SMA100A / R&S® SMF100A have to be performed.

Information Storage in the R&S® SMA100A / R&S® SMF100A Signal Generator

DATA	SDRAM	FLASH	EEPROM	REMOVABLE COMPACT FLASH MEMORY
Temporary Information storage for the CPU (CPU, Cache and Swap Area)	N			N
Hardware Information Serial Number Product Options and Calibration Correction Constants Operation Time Power On Count Relays switching Count		N	N	
BIOS and Module Relevant Data such as the module serial number and options		N	N	
Operating System and Instrument Firmware				N
Instrument states and setups, for user frequencies and levels				N

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 FLASH memories; hence, it is deemed that they do not pose a risk either.

The removable CompactFlash™ Memory card is the only device that does not lose its memory when power is removed and can contain user data. It can be removed from the signal generator leaving the customer assured that no user data is stored within the signal generator. The R&S® SMA100A / R&S® SMF100A signal generator can be equipped with this option.

The R&S® SMA100A / R&S® SMF100A Signal Generators equipped with the REMOVABLE COMPACT FLASH MEMORY (Option R&S® SMA-B80 / R&S® SMF-B85) address the needs of customers working in highly sensitive areas.

When using the R&S® SMA100A / R&S® SMF100A outside a secure area the Spare CompactFlash™ Memory card (R&S® SMA-Z10 / R&S® SMF-Z10) is recommended (see Chapter "Types of Memory in the R&S® SMA100A / R&S® SMF100A and its Security Concerns")

Performing Service, Calibration and Maintenance on the Signal Generator R&S® SMA100A / R&S® SMF100A

R&S® SMA100A / R&S® SMF100A Signal Generators equipped with the REMOVABLE COMPACT FLASH MEMORY

Turn-off the signal generator and remove the **classified** CompactFlash™ Memory card (with the user data). This removes all user data from the signal generator. The signal generator, without the removable CompactFlash™ Memory card, can now leave the secured area. Once the signal generator is outside the secured area, installing a second **non-classified** removable CompactFlash™ Memory card (without any user data; Spare CompactFlash™ Memory card R&S® SMA-Z10 / R&S® SMF-Z10), allows the signal generator to function properly for service or other needs. Prior to re-entering the secured area, the **non-classified** removable CompactFlash™ Memory card (without the user data), is removed. When the signal generator is back within the secured area, the original **classified** CompactFlash™ Memory card can be reinstalled.

To hold classified user data in the secure areas, Rohde & Schwarz recommends the REMOVABLE COMPACT FLASH MEMORY Option R&S® SMA-B80 / R&S® SMF-B85.

Calibration and the validity of the signal generator's calibration after exchange of the REMOVABLE COMPACT FLASH MEMORY

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

The EEPROM is the only location used to hold permanent adjustment values required to maintain the validity of the signal generator's calibration. Hence, replacing one removable compact flash memory with another, does not affect the validity of the instrument's calibration

After an exchange of the removable CompactFlash™ Memory card, the "internal adjustment" has to be executed once. This is done with the "Setup/internal adjustment – Adjust All" function. This function uses an internal measurement algorithm to produce the temporary adjustment values. Using the permanent and temporary values, which are then stored on the CompactFlash™ Memory card. Rohde & Schwarz recommends that users perform the internal adjustment function on a weekly basis after the signal generator has had sufficient time to warm-up.

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® SMA100A / R&S® SMF100A 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.

Firmware updates do neither change any of the passwords nor LAN or USB port enable/disable setting states.

Types of used Passwords

There are three types of passwords available in the R&S® SMA100A / R&S® SMF100A:

- User Pssword
- VNC Password
- Security Password

All three passwords are stored on the CompactFlash™ Card of the R&S® SMA100A / R&S® SMF100A.

User Password

The user password allows accessing the R&S® SMA100A / R&S® SMF100A via SSH (= Secure Shell).

Predefined user name: root

Predefined password: root

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

VNC Password

The user password allows accessing the R&S® SMA100A / R&S® SMF100A via the virtual network control software VNC.

Predefined password: instrument

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

Security Password

The security password allows enabling/disabling the LAN or USB ports of the R&S® SMA100A / R&S® SMF100A.

Predefined password: 123456
(Only digits [0 to 9] are allowed here)

In security sensitive areas it is recommended to change this 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® SMA100A / R&S® SMF100A 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. When deactivated no USB mass storage device can be connected. 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 CompactFlash™ Card.

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® SMA100A / R&S® SMF100A 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 CompactFlash™ Card.

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