R&S®ZVAX-TRM
Extension Unit
Instrument Security Procedures

1177.6030.02 ─ 02

ROHDE&SCHWARZ

Contents

1 Overview

In many cases, it is imperative that the R&S ZVAX-TRM Extension Units 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 ZVAX-TRM. 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: Extension Unit models

Product name	Order number
R&S ZVAX-TRM24	1322.6500.24
R&S ZVAX-TRM40	1322.6500.40
R&S ZVAX-TRM50	1322.6500.50
R&S ZVAX-TRM67	1322.6500.67

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 ZVAX-TRM

The Extension Unit 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.

Memory type	Size	Content	Volatility	User Data	Sanitization procedure
SRAM (CPU board)	100 kbyte	Temporary information storage for operating system and instrument firmware	Volatile	Yes	Turn off instrument power
ROM	16 kbyte	Boot loader	Non-volatile	No	None required (no user data)
Flash (microcontroller)	512 kbyte	• Hardware information: – Serial number – Product options • Operating system • Instrument firmware • Relay states (signal path) • Relay cycle counts (for maintenance purposes)	Non-volatile	No	None required (no user data)

4.1 Volatile Memory

The volatile memory in the instrument does not have battery backup. It loses its contents as soon as 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 NISPOM.

SRAM

The SRAM on the CPU board has a size of 100 kbyte and contains temporary information storage for operating system and instrument firmware. The SRAM loses its memory as soon as power is removed.

Sanitization procedure: Turn off instrument power

4.2 Non-Volatile Memory

The R&S ZVAX-TRM contains various non-volatile memories. None of these contain user data.

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

ROM

The R&S ZVAX-TRM is equipped with 16 kbyte of read-only memory for the boot loader. The ROM does not hold user data nor can the user access the storage.

Sanitization procedure: None required (no user data)

Flash

The microcontroller ATMEL SAM3 series is equipped with 512 kbyte of Flash memory.

The Flash memory on the microcontroller stores the following information:

- Hardware information, such as serial number and product options
- Operating system and instrument firmware
- Relay states (signal path)
- Relay cycle counts (for maintenance purposes)

It does not store measurement-specific data such as frequency settings, power settings or measurement results.

The Flash memory does not hold user data nor can the user access the Flash memory.

Sanitization procedure: None required (no user data)

5 Instrument Declassification

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

► Turn off the Extension Unit. This will sanitize the volatile memory.

Following this step removes all user data from the Extension Unit. The Extension Unit can now leave the secured area.

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

6 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.

Once the R&S ZVAX-TRM is connected to the network analyzer R&S®ZVA/ZVT via the type B USB connector on the rear panel of the Extension Unit, the USB type A connectors are functionally equivalent to the USB type A connectors of the network analyzer (USB hub functionality).

Disabling USB ports for writing user data

You can disable the write capability on the USB ports of the R&S ZVAX-TRM via a utility software which needs to be installed on the R&S®ZVA/ZVT. This utility software is available on the R&S®ZVA website http://www.rohde-schwarz.com/product/zva.html.

To disable the write capability, copy the utility software to the R&S®ZVA/ZVT and run it once. After a reboot of the instrument, the write capability on any USB memory device is disabled including the R&S ZVAX-TRM USB ports.

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

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