R&S®ZVA
Vector Network Analyzer
Instrument Security Procedures

ROHDE&SCHWARZ

Contents

1   Overview

In many cases, it is imperative that the R&S ZVA Vector Network Analyzers 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 ZVA. 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: Vector Network Analyzer models

Product name	Order number
R&S ZVA8 - 2 port	1145.1110.08
R&S ZVA8 - 4 port	1145.1110.10
R&S ZVA24 - 2 port	1145.1110.24
R&S ZVA24 - 4 port	1145.1110.26
R&S ZVA24 - 4 port, 4 internal sources	1145.1110.28
R&S ZVA40 - 2 port	1145.1110.40 1145.1110.43

Product name	Order number
R&S ZVA40 - 4 port	1145.1110.42
	1145.1110.45
R&S ZVA40 - 4 port, 4 internal sources	1145.1110.48
R&S ZVA50 - 2 port	1145.1110.50
R&S ZVA50 - 4 port	1145.1110.52
R&S ZVA67 - 2 port	1305.7002.02
R&S ZVA67 - 4 port, 4 internal sources	1305.7002.04
R&S ZVA110 - 2 port	1312.7004.03

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 ZVA

The Vector Network Analyzer 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
SDRAM (CPU board)	512 Mbyte up to 8 Gbyte	Temporary information storage for operating system and instrument firmware	Volatile	Yes	Turn off instrument power
SSRAM (Net-Con board)	2 Mbit x 36 bit per port	Sweep control parameters	Volatile	Yes	Turn off instrument power
EEPROM (board assembly)	256 bytes up to 1 Mbyte	Hardware information: • Serial number • Product options • Calibration correction data	Non-volatile	No	None required (no user data)
Flash (CPU board)	512 kbyte up to 4 Mbyte	BIOS	Non-volatile	No	None required (no user data)
Compact Flash (removable) or Hard Disk (removable)	4 Gbyte 500 Gbyte	• Operating system • Instrument firmware • Instrument states and set-ups • Limit lines and transducer tables • Trace data • Measurement results and screen images	Non-volatile	Yes	Remove Compact Flash memory from instrument or Remove Hard Disk from instrument

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.

SDRAM

The SDRAM on the CPU board has a size of 512 Mbyte up to 8 Gbyte and contains temporary information storage for operating system and instrument firmware. The SDRAM loses its memory as soon as power is removed.

Sanitization procedure: Turn off instrument power

SSRAM

The SSRAM on the NetCon board has a size of 2 Mbit x 36 bit per port and contains sweep control parameters. The SSRAM loses its memory as soon as power is removed.

Sanitization procedure: Turn off instrument power

4.2 Non-Volatile Memory

The R&S ZVA contains various non-volatile memories. Out of these, the removable Compact Flash memory or the removable Hard Disk contain user data. The Compact Flash memory or the Hard Disk can be physically removed from the R&S ZVA and left in the secure area.

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

EEPROM

Each board assembly in the R&S ZVA Vector Network Analyzer has one serial EEPROM device with a size of 256 bytes up to 1 Mbyte. The EEPROM contains information related to the installed hardware, such as board serial number, product options and calibration 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

The CPU board of the R&S ZVA Vector Network Analyzer has one 512 kbyte up to 4 Mbyte Flash memory device. It contains the BIOS. The Flash memory does not hold user data nor can the user access the Flash memory.

Sanitization procedure: None required (no user data)

Compact Flash memory/Hard Disk

The R&S ZVA Vector Network Analyzer can be equipped with either a Hard Disk (removable or non-removable) or a Compact Flash memory (removable). The Hard Disk and Compact Flash memory hold user data and are non-volatile. Hence, user data is not erased when power is removed from the instrument.

The removable Compact Flash memory (R&S ZVAB-B18 model .02 or .03) or the removable Hard Disk (R&S ZVAB-B18 model .04, .05 or .06) can be removed from the

Vector Network Analyzer to make sure that no user data is stored within the Vector Network Analyzer.

The R&S ZVA Vector Network Analyzer, equipped with the removable Compact Flash memory (R&S ZVAB-B18) or the removable Hard Disk, addresses the needs of customers working in secured areas.

Sanitization procedure: Remove Compact Flash memory or Hard Disk from instrument

5 Instrument Declassification

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

1. Turn off the Vector Network Analyzer. This will sanitize the volatile memory.

2. Remove the classified Compact Flash memory or the classified removable Hard Disk (containing user data).

Following these steps removes all user data from the Vector Network Analyzer. The Vector Network Analyzer can now leave the secured area.

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

Once the Vector Network Analyzer is outside the secured area, installing a second non-classified removable Compact Flash memory or removable Hard Disk (without any user data) allows the Vector Network Analyzer to function properly for service or other needs.

Prior to re-entering the secured area, the non-classified removable Compact Flash memory or removable Hard Disk (without the user data) is removed. When the Vector Network Analyzer is back within the secured area, the original classified removable Compact Flash memory or removable Hard Disk can be reinstalled.

- To hold classified user data in secure areas, use the removable Compact Flash memory or the removable Hard Disk (R&S ZVAB-B18) which comes with the instrument.
- To hold non-classified user data in non-secure areas, use a second Compact Flash memory or removable Hard Disk (R&S ZVAB-B19).

Validity of instrument calibration after declassification

The calibration makes sure that measurements comply to government standards. Rohde & Schwarz recommends that you follow the calibration cycle suggested for your instrument.

The EEPROM is the only memory type used to hold permanent adjustment values required to maintain the validity of the R&S ZVA's calibration. Therefore, replacing one removable Compact Flash memory or removable Hard Disk with another, does not affect the validity of the instrument's calibration.

Factory calibration data:

There is an individual factory calibration data set stored on each instrument which is used when no special calibration is performed. This calibration data set has been taken in the factory and consists of two files `factory.cal` and `factory.dat`.

These files are stored on the removable Compact Flash memory or on the removable Hard Disk in the directory:

```
C:\Documents and Settings\All Users\Aplication Data\
Rohde&Schwarz\Nwa\Data\calibration
```

When it is necessary to use the factory calibration in the secured area, those two files must be transferred from the non-classified to the classified removable Compact Flash memory or removable Hard Disk the first time the network analyzer returns from the service.

When there is always an individual calibration performed, no action is necessary.

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.

Disabling USB ports for writing user data

You can disable the write capability on the USB ports of the R&S ZVA via a utility software. 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 and run it once. After a reboot of the instrument, the write capability on any USB memory device is disabled.

If the USB ports are disabled for USB memory devices, it is not possible to store any user characterization data on a Calibration Unit R&S®ZV-Z5x.

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