E5072A Security Features

Rev. 2.0

October 2014

Contacting Keysight Sales and Service Offices

Assistance with test and measurements needs and information on finding a local Keysight office is available on the internet at, *http://www.keysight.com/find/assist*. If you do not have access to the internet, please contact your field engineer.

Product Declassification and Security

Model Number(s): E5072A
Product Name: ENA Series Network Analyzer
Product Family Name: ENA 7 Series

This document describes instrument security features and the steps to declassify an instrument through memory sanitization or removal. For additional information please go to **www.keysight.com/find/ad** and click on the security instrument tab.

Table of Contents

Terms and Definitions

Definitions:

Clearing – Clearing is the process of eradicating the data on media before reusing the media so that the data can no longer be retrieved using the standard interfaces on the instrument. Clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.

Sanitization – 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 to the factory for calibration. (The instrument is declassified) Keysight memory sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are outlined in the "Clearing and Sanitization Matrix" issued by the Cognizant Security Agency (CSA) and referenced in National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22M ISL 01L-1 section 8-301.

Security Erase – Refers to either the clearing or sanitization features of Keysight instruments.

Instrument declassification – A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment such as is the case when the instrument is returned for calibration. Declassification procedures will include memory sanitization and or memory removal. Keysight declassification procedures are designed to meet the requirements specified by the DSS NISPOM security document (DoD 5220.22M chapter 8)

Instrument Memory

This section contains information on the types of memory available in your instrument. It explains the size of memory, how it is used, its location, volatility, and the sanitization procedure.

Summary of instrument memory - base instrument

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
Main Memory (RAM) 2GB	Yes	No	Windows Operating system memory	Operating system (not user)	Digital Mother Board	Cycle power
Media Storage (Hard Disk Drive) 160 GB	Yes	Yes	Windows Operating system boot device, factory correction data, service log, and users file including saved traces data, settings, or images.	User-saved data	HDD assembly in the instrument (Option 019) or Removable Hard Disk Drive (Option 017)	Remove
Memory for PCI and DSP (RAM) 2.5MB	Yes	No	Data Processing for measurement	Measurement (not user)	A51 PCI DSP Card	Cycle power
Non-volatile memory (Flash) 1MB	No	Yes	Product serial number, options, correction constants, offsets, DAC values	Adjustment program performed by Keysight factory personnel or by calibration labs	A51 PCI DSP Card	N/A (The data is not stored by user under normal operation.)
Non-volatile memory (EEPROM) 32 kB	No	Yes	Board serial number, manufacturing data such as the test date	None by user.	A81 Vernier A91 Synthesizer, A2 Reciever	N/A (The data is not stored by user under normal operation.)

Memory Clearing, Sanitization and/or Removal Procedures

This section explains how to clear, sanitize, and remove memory from you instrument for all memory that can be written to during normal operation and for which the clearing and sanitization procedure is more than trivial such as rebooting your instrument.

<Memory type>

Description and purpose	Main Memory (RAM) 1GB for Windows Operating system memory
Size	1GB
Memory clearing	Power rebooting. This is a volatile memory.
Memory sanitization	Power rebooting. This is a volatile memory.
Memory removal	This memory can not be removed without damaging the instrument
Write protecting	N/A
Memory validation	N/A
Remarks	

Description and purpose	Media Storage (Built-in Hard Disk) for Windows Operating system boot device, factory correction data, service log, and users file including saved traces data, settings, or images.
Size	160 GB
Memory clearing	N/A
Memory sanitization	N/A
Memory removal	Built-in hard disk is removable. Refer to the below note for the detail information for remove/replace/re-store the disk.
Write protecting	N/A
Memory validation	N/A
Remarks	

Hard Disk removal: Because it is virtually impossible to completely and selectively erase all user data on a hard drive without also destroying the operating system, the best method for maintaining security when the ENA must be removed from a secure area is to replace the hard drive with a "non-secure" hard drive, i.e. a drive that has never had any sensitive data placed on it. This allows the ENA to still function properly in non-secured areas or for use when servicing.

E5072A-017 has an easily accessible hard drive on the rear panel. Keysight has available a relatively inexpensive, pre-configured hard drive for the ENA that must be purchased in order for this security method to work.

For Option 019 User:
Before taking the following steps, Option 019 user must be applied the E5072AU-217 (UPGADE TO REMOVABLE HARD DISK DRIVE).

Hard disk removal: Step-by-step procedure
These steps should be followed to maintain security:

1. Purchase the Hard Disk Drive Kit (E5072AU- 028). Clearly mark this hard drive as "Unsecured!". In the event the secure ENA needs to be used elsewhere, or, if it needs servicing:
2. Copy the files with .lic extension into your USB memory (or network shared directory). The files have option information.
3. Remove the secure hard drive (label it as secured if desired) and keep it in a secured area.
4. Remove the ENA from the secured area and install the "unsecured" hard drive.
5. Connect the external keyboard and mouse to the connectors on the ENA. Then, turn on the ENA.

6. Press [Macro Setup] and press Load Project... in the softkey menu.
7. A dialog box appears for you to select the program to be loaded. Select RestoreSysCorFile.vba from the D:\Agilent\Service folder and then press the Open button.
8. Press [Macro Run]. The RestoreSysCorFile dialog box appears. Then click OK.
9. Place the *.lic files into the directory named E:\License. If there is no License directory, create it.

The ENA can now be used elsewhere or sent for servicing without fear of leaking any sensitive information.

Hard disk re-installation: Step-by-step procedure
When the ENA needs to be returned to the secured area, follow the steps listed below. Any servicing of the ENA may include the regeneration of correction constants.

1. Remove the unsecured hard drive, transport the ENA to the secured area, and replace the hard drive with the secured version
2. Connect the external keyboard and mouse to the connectors on the ENA. Then, turn on the ENA.
3. Press [Macro Setup] and press Load Project... in the softkey menu.
4. A dialog box appears for you to select the program to be loaded. Select RestoreSysCorFile.vba from the D:\Agilent\Service folder and then press the Open button.
5. Press [Macro Run]. The RestoreSysCorFile dialog box appears. Then click OK.
6. Place the *.lic files which you stored in the step 2 in the hard disk removal into the directory named E:\License. If there is no License directory, create it.

Note: If your secured HDD does not have the “RestoreSysCorFile.vba” program on it, copy the program from the unsecured HDD.

Description and purpose	Memory for PCI and DSP (RAM)
Size	2.5 MB
Memory clearing	Power rebooting. This is a volatile memory.
Memory sanitization	Power rebooting. This is a volatile memory.
Memory removal	This memory can not be removed without damaging the instrument
Write protecting	N/A
Memory validation	N/A
Remarks	

Description and purpose	Non-volatile memory (Flash) for Product serial number, options, correction constants, offsets, DAC values
Size	1 MB
Memory clearing	Adjustment program performed by Keysight factory personnel or by calibration labs only.
Memory sanitization	Adjustment program performed by Keysight factory personnel or by calibration labs only.
Memory removal	This memory can not be removed without damaging the instrument
Write protecting	N/A
Memory validation	N/A
Remarks	The data is not stored by user under normal operation.

Description and purpose	Non-volatile memory (EEPROM) for board serial number, manufacturing data such as the test date.
Size	32 kB
Memory clearing	None by customer
Memory sanitization	None by customer
Memory removal	This memory cannot be removed without damaging the instrument
Write protecting	N/A
Memory validation	N/A
Remarks	The data is not stored by user under normal operation.

User and Remote Interface Security Measures

Screen and Annotation Blanking

The frequency-blanking feature is available. This function provides three security levels:
"OFF" during normal operation;
"Low" deletes frequency information from the display, but can be turned "OFF" by front panel operation; and
"High" deletes frequency information from the display, and cannot be turned "OFF" except rebooting.

The operator can perform the following keystrokes to control this frequency-blanking feature,
[System] > Service Menu > Security Level > None|Low|High,

or set the levels by the following SCPI command:
:SYSTem:SECurity:LEVel {NONE|LOW|HIGH}

Note:
Any SCPI/COM commands that read the frequency data are not influenced by this function. All commands can read frequency data regardless of the security level.

USB Mass Storage Device Security

Users can disable any USB-compatible external mass storage devices in order to ensure confidentiality. The following procedure shows how to disable a USB Mass Storage Device.

1. [Save/Recall] > Explorer….
2. Double-click "DisableUsbStorage.exe" from D"\Agilent\Service.
3. Click OK in the SUCCEEDED message window that appears. If any USB mass storage device is connected to the E5072A under this condition, the Hardware Wizard will start, but the USB mass storage device will not work.

The following procedure shows how to enable a USB Mass Storage Device.

1. [Save/Recall] > Explorer….
2. Double-click "EnableUsbStorage.exe" from D"\Agilent\Service.
3. Click OK in the SUCCEEDED message window that appears.

Note: If you do not want any USB mass storage device to ever be enabled at any time, delete EnableUsbStorage.exe from the E5072A after DisableUsbStorage.exe has been completed. These two programs will not be recovered automatically by applying the firmware update or other such action. Before

deleting any of these programs, you should make a backup copy to a recording medium such as a floppy disk and store it separately.

Note: If the program fails to run, it is possible that you have not logged in as a user in the Administrators Group. When you want to execute any of the above programs, make sure to log in as a user in the Administrators Group.

Remote Access Interfaces

The user is responsible for providing security for the I/O ports for remote access by controlling physical access to the I/O ports. The I/O ports must be controlled because they provide access to all user settings, user states and the display image.
The I/O ports include USB, GPIB and LAN.
The LAN port provides the following services, which can be selectively disabled:
http
ftp
sockets
telnet
There is also a 'ping' service, which presently cannot be selectively disabled. The concern here might be that it is possible to discover IP addresses of connected instruments in order to query their setups over the net or break into the code.

Procedure for Declassifying a Faulty Instrument

To declassify an ENA if it needs to be removed from a secure area, follow the procedure for "Hard disk removal. Step-by-step procedure" on page 5.

When the ENA needs to be returned to the secure area, follow the procedure for "Hard disk re-installation. Step-by-step procedure" on page 6.