E4982A Security Feature

Rev. 2.0

October 2014

Copyright 2012, 2014 Keysight Technologies

Contacting Keysight Sales and Service Offices

Assistance with test and measurements needs and information on finding local Keysight offices are 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.

Note: In any correspondence or telephone conversations, refer to the signal generator by its model number and full serial number. With this information, the Keysight representative can determine whether your unit is still within its warranty period.

Product Declassification and Security

Model Number(s): E4982A
Product Name: LCR Meter
Product Family Name: LCR Meter

This document describes instrument security features and the steps to declassify an instrument through memory sanitization or removal.

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. 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 – Security erase is a term that is used to refer 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 (DRAM) 2GB	Yes	No	Windows Operating system memory	Operating system (not user defined)	A60 CPU Module	Cycle power
Media Storage (Hard Disk Drive) 160 GB	Yes	Yes	Windows Operating system boot device, factory correction data, and users file including saved traces data, settings, or images.	User-Saved Data Operating system (not user defined)	HDD assembly	Remove
Memory for DSP module (RAM) 1.8M bit	Yes	Yes	Data Processing for measurement	Measurement (not user defined)	A51 DSP Module	Cycle power
Non-volatile Memory (Flash) 512M Bit	No	Yes	Product serial number, Options, System calibration (correction constants) data (not user defined calibration data)	Adjustment Program performed by Keysight factory personnel or by calibration labs	A51 DSP Module	N/A (The data is not stored by user under normal operation.)
Non-volatile Memory (EEPROM) 256M Bit	No	Yes	Module serial number, Revision number	Calibration at factory	A11 Source Module A6 Receiver Module	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 your instrument for all memory types.

<Memory type>

Description and purpose	Main Memory for Windows Operating system memory
Size	2 GB
Memory clearing	Power rebooting. This is a volatile memory.
Memory sanitization	Power rebooting. This is a volatile memory.
Memory removal	This memory cannot be removed without damaging the instrument
Write protecting	N/A
Memory validation	N/A
Remarks	

Description and purpose	Media Storage (Hard Disk Drive)
Size	160 GB
Memory clearing	N/A
Memory sanitization	N/A
Memory removal	The hard disk drive needs to be removed and replaced with a new or unused hard disk drive part as per the Replacement Procedure/Parts List. See E4982A Replacement Procedure/Parts List for more detail information on the procedure as well as the replacement parts.
Write protecting	N/A
Memory validation	N/A
Remarks	

Description and purpose	Memory for DSP (RAM) for A51 DSP Module
Size	1.8M bit
Memory clearing	Power rebooting. This is a volatile memory.
Memory sanitization	Power rebooting. This is a volatile memory.
Memory removal	This memory cannot be removed without damaging the instrument.
Write protecting	N/A
Memory validation	N/A
Remarks	

Description and purpose	Non-volatile memory (Flash) for A51 DSP Module. This memory is for product serial number, option and system calibration data (Any user data is not stored in these memory)
Size	512M Bit
Memory clearing	N/A
Memory sanitization	N/A
Memory removal	The A51 DSM module needs to be removed and replaced with a new or unused module as per the Replacement Procedure/Parts List. See E4982A Replacement Procedure/Parts List for more detail information on the procedure as well as the replacement parts.
Write protecting	N/A
Memory validation	N/A
Remarks	

Description and purpose	Non-volatile memory (EEPROM) for A1 and A6 Modules. These memories are for board serial number, board revision number. (Any user data is not stored in these memories)
Size	256 M Bit
Memory clearing	N/A
Memory sanitization	N/A
Memory removal	The A1 and A6 modules need to be removed and replaced with a new or unused module as per the Replacement Procedure/Parts List. See E4982A Replacement Procedure/Parts List for more detail information on the procedure as well as the replacement parts.
Write protecting	N/A
Memory validation	N/A
Remarks	

User and Remote Interface Security Measures

Screen Blanking

The operator can perform the following keystrokes to make the screen blank.
[Display] > Display

Or, execute the following SCPI command:
:DISPlay[:WINDow]:TEXT1[:STATe] {ON|OFF|1|0}

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 E4982A 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 E4982A 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:

a) http
b) ftp
c) sockets
d) telnet

There is also a 'ping' service, which presently cannot be selectively disabled. The concern 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.