

Security Features and Volatility Documentation

Keysight Technologies, Inc.

Model Numbers:

34460A

34461A

34465A

34470A

Product Family:

Truevolt Series of Digital Multimeters



5991-1950EN
Revision 2.0
January, 2015
© Keysight Technologies, Inc. 2013 - 2015

Contents

Introduction	4
Contacting Keysight Sales and Service Offices	4
Product Declassification and Security	4
Terms and Definitions.....	5
Instrument Memory and Volatility Information	6
Memory Clearing, Sanitization and/or Removal Procedures.....	11
User and Remote Interface Security Measures	13
Procedure for Declassifying a Faulty Instrument	17

Introduction

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/security or www.keysight.com/find/ad and click Instrument Security in the Related Links area.

Contacting Keysight Sales and Service Offices

Assistance with test and measurement needs, and information to help you find a local Keysight office, is available at www.keysight.com/find/assist. Otherwise, please contact your designated Keysight representative.

Note: In any correspondence or telephone conversation, refer to the instrument 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 Numbers:

34460A, 34461A, 34465A, 34470A

Product Name:

34460A – Digital multimeter, 6½-digit, basic Truevolt DMM

34461A – Digital multimeter, 6½-digit, 34401A replacement, Truevolt DMM

34465A – Digital multimeter, 6½-digit, Truevolt DMM

34470A – Digital multimeter, 7½-digit, Truevolt DMM

Product Family Name:

Truevolt Series of Digital Multimeters

Terms and Definitions

Clearing

As 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 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.

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 include memory sanitization or memory removal, or both. Keysight declassification procedures are designed to meet the requirements specified in DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)”, Chapter 8.

Sanitization

As 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 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 specified in the “Clearing and Sanitization Matrix” in Appendix O of the ODAA Process Guide for C&A of Classified Systems under NISPOM.

Secure Erase

Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight instruments.

Instrument Memory and Volatility Information

This section contains information on the types of memory available in your instrument, including the memory size, usage, location, volatility, and sanitization procedure.

This instrument uses one NAND Flash memory chip to retain the needed system information and the user memory partition. The User memory partition is separate and independent so that the sanitization procedures may be applied to only this partition on a sector by sector basis.

Performing an instrument sanitization requires the instrument Security option (SEC) to be installed. Please refer to the *Truevolt Series Operating and Service Guide* for more information on available options.

Summary of instrument memory - base instrument

Memory Type and Size	User accessible as a mass storage device?	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
System Flash (NAND Flash) 45 MB	No	Yes	Yes	Contains operating system, instrument firmware, and the firmware recovery image	Factory Install / Firmware Upgrade	Front panel U203 1819-0707 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
User Flash (NAND Flash) 80 MB	Yes	Yes	Yes	User data, configuration and preference files, screen capture files, instrument state files, and user reading storage	User-saved data	Front panel U203 1819-0707 (same chip as other parts, but managed separately)	NAND Flash Sanitize – See Table 1
Calibration Store (NAND Flash) 3 MB	No	Yes	Yes	Calibration constants, calibration count, secure count, security code, and calibration message	Factory or Service and user calibration	Front panel U203 1819-0707 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.

Memory Type and Size	User accessible as a mass storage device?	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
Front panel microprocessor (Flash) 8 kB	No	No	Yes	Front panel microprocessor execution code storage	Factory Install / Firmware Upgrade	Front panel microprocessor U401 1822-3182 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Front panel microprocessor (EEPROM) 512 Bytes	No	Yes	Yes	Stores instrument ON/OFF power state (not the power-on configuration)	Operating System or Microprocess or execution code	Front panel microprocessor U401 1822-3182 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Front panel microprocessor (RAM) 256 Bytes	No	Yes	No	Front panel microprocessor temporary execution data	Microprocess or execution code	Front panel microprocessor U401 1822-3182 (same chip as other parts, but managed separately)	Power cycle
Main processor (ROM) 32 kB	No	No	Yes	Main processor execution code	Manufacturer programmed	Front panel U201 1822-4268 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.

Memory Type and Size	User accessible as a mass storage device?	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
Main processor (SRAM) 8 kB	No	Yes	No	Temporary execution data	Operating System	Front panel U201 1822-4268 (same chip as other parts, but managed separately)	Power cycle
Main RAM (SDRAM) 1 G-bit	No	Yes	No	Temporary execution data	Operating System	Front panel U204 1819-0389	Power cycle
Measurement Processor (Flash) 512 kB	No	No	Yes	Processor execution code	Factory Install / Firmware Upgrade	Main board U901 1822-4407 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Measurement Processor (SRAM) 98 kB	No	Yes	No	Data path processing	Measurement Processor Flash	Main board U901 1822-4407 (same chip as other parts, but managed separately)	Power cycle

Memory Type and Size	User accessible as a mass storage device?	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
Measurement Processor (ROM)	No	No	Yes	Processor execution data	Manufacturer programmed	Main board U901 1822-4407 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Measurement Calibration (EEPROM) 64 k-bit	No	Yes	Yes	Calibration data	User calibration	Main board U904 1819-0623	N/A, contains no application-specific information.
Measurement FPGA (Flash) 1.27 M-bit	No	No	Yes	Logic Array Configuration	Factory Install / Firmware Upgrade	Main board U803 1822-3758	N/A, contains no application-specific information.
Measurement FPGA (SRAM) 166 k-bit	No	Yes	No	Data processing	Measurement FPGA Flash	Main board U803 1822-3758	Power cycle

Summary of instrument memory: 34460A-GPB, 34461A-GPB, 34465A-GPB, 34470A-GPB, 3446GPBU

Memory Type and Size	Is Memory user accessible as a mass storage device?	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
FPGA 1M-bit	No	Yes	Yes	Control interface between main processor and GPIB	Flash Memory	GPIB interface 1822-1960	N/A, contains no application-specific information.
Flash 1M-bit	No	No	Yes	Stores GPIB control FPGA program bits	Factory Install / Preprogrammed part	GPIB interface P0001-80001	N/A, contains no application-specific information.

Memory Clearing, Sanitization and/or Removal Procedures

This section explains how to clear, sanitize, and remove memory from your instrument for all memory that may contain application-specific information and that can be written to during normal operation. This section also highlights the clearing and sanitization procedures if more than trivial, such as cycling power on your instrument.

Performing an instrument sanitization requires the instrument Security option (SEC) to be installed. Please refer to the *Truevolt Series Operating and Service Guide* for more information on available options.

With the instrument Security option, a single button press will completely sanitize all internal user accessible memories using the appropriate NISPOM sanitization procedure. Without this option, user files must be individually deleted or overwritten to manually clear memory.

User Flash (NAND Flash)

Table 1

Description and purpose	This is the user’s partition of internal storage that uses a NAND flash device. Storage may include instrument configuration, preference and state files, screen capture images, and user reading storage for measurement results.
Size	80 MB
Memory clearing	<p>To remove individual files from the file system on the front panel press: [Utility] > Manage Files > Action > Delete > Browse. Then select the file and press Select > Perform Delete > Yes.</p> <p>To remove all files from the file system on the front panel press: [Utility] > Manage Files > Action > Delete > Browse. Then select Internal and press Select > Perform Delete > Yes.</p> <p>To remove files and folders from the file system via the remote interface, use: MMEemory:DELeTe {<file> <filespec>} MMEemory:RDIRectory <folder></p> <p>See the <i>Truevolt Series Operating and Service Guide</i> for more information.</p>
Memory sanitization	<p>Performing an instrument sanitization requires the instrument Security option (SEC) to be installed. Please refer to the <i>Truevolt Series Operating and Service Guide</i> for more information on available options.</p> <p>***** Requires Instrument Security Option *****</p> <p>On front panel press: [Utility] > Test/Admin > Security > NISPOM Sanitize > Sanitize</p> <p>From the remote interface, send: SYSTem:SECurity:IMMediate</p> <p>Note: The instrument’s security setting must be unlocked to perform these actions. Executing a sanitize operation will increment the instrument’s secure count.</p> <p>This sanitizes all user-accessible instrument memory and restarts the instrument. This includes deleting and sanitizing all measurement data, user-defined state or preference information, and user-defined I/O settings. The instrument’s firmware, serial/model number, and calibration data are preserved.</p> <p>This command complies with requirements in chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specifically, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.</p> <p>See the <i>Truevolt Series Operating and Service Guide</i> for more information.</p>
Memory removal	This memory cannot be removed without damaging the instrument. The user may remove the front panel assembly on which the memory chip resides. Remove the front panel board per the disassembly instructions in the <i>Truevolt Series Operating and Service Guide</i> .

User and Remote Interface Security Measures

How to determine if the instrument's Security option is installed

From the front panel, press:

[Help] > About

From the remote interface, send:

*OPT?

A string containing "SEC" will be returned if the instrument Security option is installed.

Administrative Password

To defeat or override an instrument's administrative password (calibration secure override/Security option override) follow the procedure in the *Truevolt Series Operating and Service Guide*. This involves removing power and other connections to the instrument, removing the instrument cover (requires tools), shorting a jumper, and cycling power. The calibration count and secure count will increment when the password is defeated using this method.

When setting a new password, the password must begin with a letter and contain 1 to 12 letters (A-Z), digits (0-9), or underscores (_).

The password never expires.

This instrument does not track or report invalid password attempts, nor does it lock-out password entry following a number of invalid password entries.

Managing Remote Interface Access

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.

With the instrument Security option, modifying these settings requires the instrument password. The secure count will increment when a remote interface is disabled or enabled. See the *Truevolt Series Operating and Service Guide* for more information.

The LAN port provides the following services, which can be selectively disabled:

- a) LAN
- b) VXI-11
- c) Sockets
- d) Telnet
- e) Web
- f) mDNS
- g) HiSLIP

To disable LAN services:

On the front panel, press:

[Utility] > I/O Config > LAN Off/On, or use

[Utility] > I/O Config > LAN Settings > LAN Services, then select the interface to enable or disable

On the remote interface, use:

SYSTEM:COMMunicate:ENABLE {ON|OFF}, <interface>

For mDNS on the remote interface, use:

LXI:MDNS:ENABLE {ON|OFF}

To disable USB:

On the front panel, press:

[Utility] > I/O Config > USB Settings > USB SCPI Off/On

On the remote interface, use:

SYSTEM:COMMunicate:ENABLE {ON|OFF}, USB

To disable GPIB:

On the front panel, press:

[Utility] > I/O Config > GPIB Settings > GPIB Off/On

On the remote interface, use:

SYSTEM:COMMunicate:ENABLE {ON|OFF}, GPIB

USB Mass Storage Device Security

Not Supported

Controlling the USB device MTP (driverless) connection service

On the front panel press:

[Utility] > I/O Config > USB Settings > File Access Off/On

On the remote interface use:

SYSTEM:COMMunicate:ENABLE {ON|OFF}, USBMTP

If the instrument Security option is installed, this requires that the instrument is unlocked. The secure count will increment when this port is disabled or enabled. See the *Truevolt Series Operating and Service Guide* for more information.

Controlling the Front Panel USB Host port

On the front panel press:

[Utility] > I/O Config > USB Settings > USB Front Off/On

On the remote interface use:

SYSTEM:USB:HOST:ENABLE {ON|OFF}

This requires the instrument Security option, and that the instrument is unlocked. The secure count will increment when this port is disabled or enabled. See the *Truevolt Series Operating and Service Guide* for more information.

Controlling the Front Panel Display

To provide basic security, you may disable the front panel display.

To disable the display on the front panel, press:

[Utility] > System Setup > User Settings > Display Options > Display OFF

Note: pressing any key will enable the display again.

To disable the display on the remote interface, send:

DISP OFF

Note: pressing **Local** will enable the display again.

The display is enabled when power is cycled. See the *Truevolt Series Operating and Service Guide* for more information.

How to disable the Front Panel during remote operation

To programmatically lock out all front panel operation and remote access over the current interface, use the SYSTEM:LOCK command. See the *Truevolt Series Operating and Service Guide* for more information.

Calibration Regulation

The instrument requires a password to unsecure the instrument before calibration. The instrument's calibration count will increment with each successful calibration step.

Firmware Update Regulation

The instrument requires a password to unsecure the instrument before updating firmware. The instrument's calibration count will increment with each successful update.

Instrument Specifics

Main Processor: STMicroelectronics SPEAR320S-2, ARM9926EJ-S 333MHz 289-LFBGA

Ethernet PHY Transceiver: IEEE-802.3/ 802.3u compliant 10/100 base-T, SMSC LAN8710A

Operating System: Microsoft Windows® CE 6.0 R3

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States or other countries.

Procedure for Declassifying a Faulty Instrument

If the instrument is not functioning and the user is unable to use the security functions to declassify the instrument, the user must physically remove the front panel printed circuit assembly from the instrument. Once this assembly is removed, proceed with one of these options:

- Destroy the front panel printed circuit assembly using a DSS/NISPOM approved destruction method

OR

- Remove the NAND flash memory component located on the front panel printed circuit assembly (U203), and destroy it using a DSS/NISPOM approved destruction method

Refer to the *Truevolt Series Operating and Service Guide* procedures for removing the front panel printed circuit assembly.

Send the instrument to a Keysight repair facility. If the unit has option SEC and is still under warranty, the repair facility will replace the front panel printed circuit assembly. If this restores instrument functionality, the user will not be charged for the new assembly. If a different assembly is at fault, the user will be charged for the new front panel assembly even though the instrument is still under warranty.