PNA Security Features

This document applies to the following Agilent Network Analyzers:

- E8356A (Discontinued)
- E8357A (Discontinued)
- E8358A (Discontinued)
- E8361A
- E8362A (Discontinued)
- E8362B
- E8363A (Discontinued)
- E8363B
- E8364A (Discontinued)
- E8364B
- E8801A (Discontinued)
- E8802A (Discontinued)
- E8803A (Discontinued)
- N3381A (Discontinued)
- N3382A (Discontinued)
- N3383A (Discontinued)
- N5230A

Agilent Technologies

N5230-90023

Printed in USA

May 2005

Terms and Definitions

Clearing 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 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) Agilent 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 Agilent instruments.

Instrument Declassification 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. Agilent declassification procedures are designed to meet the requirements specified by the DSS NISPOM security document (DoD 5220.22M chapter 8)

▪

PNA Memory

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

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 (SDRAM) 64 MB to 512 MB (depending on model and vintage)	Yes	No	Firmware operating memory	Operating system (not user)	CPU board	Cycle power
Hard Disk Drive 10 GB or 40 GB depending on model and vintage.	Yes	Yes	User files, including calibrations and instrument states.	User-saved data	Most models are removable from the rear panel. (See note below).	
EEPROM 512B	No	Yes	Instrument information such as Serial number, installed options, correction constants	Factory or authorized personnel only	1, 2, or 3 EEPROMs contained on most PC Boards.	

Note: The following discontinued PNA models were shipped with hard disk drives that are removable only by removing the outer covers: E8356A, E8357A, E8358A, E8801A, E8802A, E8803A, N3381A, N3382A, N3383A.

Memory Clearing, Sanitization and/or Removal Procedures

This section explains how to clear, sanitize, and remove memory from your PNA 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.

Description and purpose	Hard Disk Drive
Size	10 GB or 40 GB depending on PNA model and vintage.
Memory clearing	Delete user files and empty recycle bin
Memory sanitization	Remove Hard Disk Drive and replace with a new or unused Hard Disk Drive. See PNA Service Manual for details.
Memory removal	Remove Hard Disk Drive
Write protecting	N/A

User and Remote Interface Security Measures

Screen and Annotation Blanking

You can prevent frequency information from appearing on the PNA screen and printouts. To set security levels from the PNA menu, click **System**, then **Security**. When the security level is set to **Low** or **High**, frequency information is blanked from the following:

- Display annotation
- Calibration properties
- All tables
- All toolbars
- All printouts
- GPIB console - When set to **None** or **Low**, nothing is blanked. When set to **High**, the GPIB console is inactive.

When the Security level is set to **Low** or **High**, frequency information is **NOT** blanked from the following:

- The Frequency Converter Application (opt 083) dialog box information or printouts.
- Service Programs.
- Your COM or SCPI programs.

USB Mass Storage Device Security

To prevent USB write capability on XPSP2, create a new registry key of: **`HKLM\System\CurrentControlSet\Control\StorageDevicePolicies`**.

Then create a **`REG_DWORD`** entry in it called **`WriteProtect`**. Set it to "**`1`**" and you'll be able to read from USB drives but not write to them

Remote Access Interfaces

The user is responsible for providing security for the I/O ports that allow 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 RS-232, GPIB, and LAN.

The LAN port provides the following services, common to all Windows-based computers, which can be selectively disabled:

- http
- ftp
- sockets
- telnet

There is also a 'ping' service, which cannot be selectively disabled. Therefore, it is possible to discover IP addresses of connected instruments in order to query their setups over the internet or break into the code.

Procedure for Declassifying a Faulty Instrument

As shipped from the factory, all PNAs have the following PNA-specific files stored on the hard disk drive. When replacing a hard disk drive, in order to achieve specified performance, these files must be copied to the new hard drive. These files all begin with **`mxcalfiles_`** and are located in the directory: `C:\Program Files\Agilent\Network Analyzer`.

Perform the following procedure to declassify a PNA if it needs to be removed from a secure area.

1. When a new PNA is received, or if this step has not yet been done, copy files that begin with "**mxcalfiles_** " from the hard disk drive to a floppy disk. This disk should be maintained in a non-secure area.
2. Purchase the appropriate spare hard drive and keep it with the above floppy disk. Clearly mark this hard drive as "Unsecured!"
3. Remove the secure hard drive from the PNA and keep it in the secured area.
4. Remove the PNA from the secured area and install the "unsecured" hard drive.
5. If not previously done, copy the mxcalfiles from the floppy disk to the directory listed above.

Perform the following procedure when the PNA needs to be returned to the secure area. Any servicing of the PNA may include the regeneration of correction constants. Most of these are contained in the on-board EEPROMs so no action is necessary. The only exception is with the mxcalfiles; see below.

1. If the PNA was sent out for servicing, check to see if any of the mxcalfiles have been updated (check the last-modified date.) If so, these updated files should be copied to a floppy disk so that they can be updated on the secured hard drive.
2. Remove the unsecured hard drive, transport the PNA to the secure area, and replace the hard drive with the secure version
3. If the mxcalfiles have changed, copy all new files saved to the floppy disk to the directory listed above.