SECURE ERASE & MILITARY PURGE ROUTINES

Application Note

Document #AN0010 – Viking Secure Erase & Military Purge | Rev. C

Table of Contents

1 Introduction

All Viking SSD's are self-encrypting drives (SED), with a bulk data encryption feature that provides automatic hardware-based AES-256 data security and enhanced secure erase capability.

A self-encrypting drive, scrambles data using a data encryption key as it is written to the drive and then descrambles it with the key as it is retrieved. This gives the user the highest level of data protection available and provides a fast erase simply by deleting the encryption key, eliminating the need for time consuming data-overwrite. Data on the drive is instantly rendered unreadable.

However data-overwrite options (Military Purge Routines) are available and described later in this document in the section "Military Secure Erase / Sanitization". Use of these Purge Routines may reduce the life of the SSD.

The SSD supports AES-256 and ATA Secure Erase features to protect sensitive data. Refer to AN0009 for more information on encryption. The drive is also available with TCG security enhancements.

The ATA Security Erase Unit command, which is usually password protected, will erase:

- All map data
- The encryption key (All data in flash is scrambled and unrecoverable)

and the resulting condition of the drive after an ATA Security Erase will be:

- Any reads to the drive will respond with zero for every LBA
- Any writes to the drive will act as if the drive has nothing; a T0 state.

If the flash memory was directly probed, some scrambled data might be retrievable, but there would be no way to decode it without the encryption key.

2 ATA Security Command Codes

The Security Mode command set consist of:

- Security Set Password (OPCODE: F1h)
- Security Unlock (OPCODE: F2h)
- Security Erase Prepare (OPCODE: F3h)
- Security Erase Unit (OPCODE: F4h)
- Security Freeze Lock (OPCODE: F5h)
- Security Disable Password (OPCODE: F6h)

3 Secure Erase Command Codes

In the following table are the supported Secure Erase Commands for the SSD.

Table 3-1: SSD Secure Erase Commands

Command	Action	SSD Code[1]	Time to Execute
Cryptographic Secure Erase	• Erase all map data • Erase encryption key • Erase all LBAs • Erase SMART attributes, logs, thresholds • Reset/Regenerate a new AES key	Note 1,2	< 4 seconds
Cryptographic Secure Erase with Flash Erase	Secure Erase actions plus the erasure of all encrypted data and blocks in flash memory	Note 1	~1 second/GB

Notes:

1. Enabled in firmware at the time of manufacture and prior to shipping from the factory
2. Factory default is Cryptographic Secure Erase (WITHOUT Flash Erase). Contact Viking for a utility to change the default.

There are two primary reasons for performing a Secure Erase on an SSD. The first and perhaps the most important is to remove ultra-sensitive data from the drive to prevent any access and ensure the privacy of information previously stored in the flash. This aspect of the secure erase is often required by some military or government agencies.

The second reason for a Secure Erase is to initialize the drive to a known starting point for benchmarking purposes or to increase performance and/or capacity by eliminating any preconditioning.

Unlike the ATA Security Erase Unit command which only erases the map data and the encryption key for the encrypted data in flash memory, the Secure Erase command will also:

- Erase all map data (and checks the drive to ensure map loss is persistent)
- Erase encryption key (All data in flash is scrambled and unrecoverable)
- Erase all LBAs (0 to MAX) in DEVICE CONFIGURATION IDENTIFY
- Erase SMART Attributes
- Erase SMART Logs
- Erase SMART Thresholds (and return to default)
- Reset and regenerate a new AES key to apply to all data

In less than 4 seconds after a Secure Erase command, scrambled encrypted data cannot be located or retrieved.

The SSD also has an optional Cryptographic Erase *plus Physical Flash Erase* command where in addition to a Secure Erase, all encrypted, unreadable data and all Flash blocks (excluding FW blocks) are erased. Persistent drive life data is rewritten to the flash blocks after erase. The operation time for a Cryptographic Erase with Physical Flash Erase, scrambled encrypted data is ~ 1 second/GByte (~2 minutes per 128GB)

4 Military Secure Erase / Sanitization

Although unnecessary with SED SSD, many government and military organizations such as NIST/NSA define their own standard and procedures for performing a Military Secure Erase which overwrite different patterns to sanitize the flash media. Some of the more common military or government purge routines are defined in the following table and the data security features of the drive comply with Department of Defense (DoD) and US military data security standards written for hard-drives (HDD).

Table 4-1: Military Secure Erase / Sanitize Routines

Standard	Action	Notes
NSA/CSS 9-12	Erase and overwrite all locations with a known unclassified pattern. Verify the overwrite procedure by randomly rereading the overwritten information to confirm that only the known pattern can be recovered.	Note 1,3
NSA/CSS 130-2	Erase the media and overwrite with random data 2 times, then erase and overwrite with a character	Note 1
DoD5220.22-M NISPOM	Erase the media and overwrite with single character, then erase again	Note 1
DoD5220.22-M NISPOM Sup 1	Erase the media and overwrite with single character, then erase again and overwrite with single character, then erase again and overwrite with random character then erase again	Note 1
USA Army 380-19	Erase the media and overwrite with random data, erase and overwrite with a character, then erase and overwrite with complement of the character	Note 1
Navy NAVSO P-5239-26	Erase the media and overwrite with random data, then erase again	Note 1
Air Force AFSSI 5020	Erase the media and overwrite with pattern, repeat 3 times	Note 1
IRIG 106-2007 IRIG 106-07, Ch. 10.8	Erase the media, overwrite with 0x55, erase, overwrite with 0xAA, and then erase again. Then fill the drive with a repeating string of Secure Erase.	N/A

Notes:

1. Enabled in firmware at the time of manufacture and prior to shipping from the factory
2. Military purge routines are user changeable. Contact Viking for a utility to perform this task.
3. NSA/CSS 9-12 is the factory default unless otherwise requested.

Table 4-2: Military Secure Erase / Sanitize Routines timings

Usable Capacity	25GB	50/55/60GB	100/115/120GB	200/235/240GB	400/480GB	Notes
Raw Capacity	**32GB**	**64GB**	**128GB**	**256GB**	**512GB**	
NSA 9-12	10 min	15 min	35 min	1:05 hrs		Note 1
NSA 130-2	25 min	40 min	1:45 hrs	3:20 hrs		
DoD 5220	Failed	Failed	Failed	Failed		
DoD 5220 Sup 1	25 min	45 min	1:45 hrs	3:30 hrs		
Army 380-19	30 min	40 min	1:45 hrs	3:30 hrs		
NAVSO 5239	30 min	40 min	1:50 hrs	3:20 hrs		
AFSSI	10 min	15 min	35 min	1:10 hrs		
Config ID	15052	15041	15010	15009	15012	

Notes:

1. NSA/CSS 9-12 is the factory default.

5 Reference Documents

- Viking SSD Product Datasheets: http://www.vikingtechnology.com
- Viking Application Note AN0009 – SSD AES Encryption
- Viking Application Note AN0026 - TCG- OPAL

6 About Viking Technology

Viking Technology develops and delivers innovative high-technology products that optimize the value and performance of our customers' applications. Founded in 1989, Viking Technology has been providing Original Equipment Manufacturers (OEMs) with industry leading designs, engineering, product support and customer service for over 25 years. For more information visit http://www.vikingtechnology.com.

7 Revision History

6/27/11		Added Military Secure Erase / Sanitize Routines timings for 32GB, 64GB, 128GB, 256GB and 512GB SATA drives
7/12/11		Added information on SED and added a reference to AN0009
9/5/17		Revise logo and address
9/21/17		Remove Element SSD. Change to "for over 25 years". Add "Use of these Purge Routines may reduce the life of the SSD." Remove AES-128. Add AES-256. Remove SMART Attributes #s. Add "Although unnecessary with SED SSD", Add reference to AN0026

Global Locations		
US Headquarters	India Office	Singapore Office
2950 Red Hill Ave. Costa Mesa, CA 92626 Main: +1 714 913 2200 Fax: +1 714 913 2202	A 3, Phase II, MEPZ-Special Economic Zone NH 45, Tambaram, Chennai-600045 India	No 2 Chai Chee Drive Singapore, 109840

For all of our global locations, visit our website under global locations. For sales information, email us at sales@vikingtechnology.com

viking TECHNOLOGY

DRAM MEMORY & FLASH STORAGE
NVDIMM, SSD, DRAM, MCP & CUSTOM
for Embedded, Industrial, Defense & Aerospace