SSD AES ENCRYPTION

Application Note

Document #AN0009 – Viking SSD AES Encryption | Rev. B

Purpose of this Document

This application note was prepared to help OEM system designers evaluate the performance of Viking solid state drive solutions by using the same benchmarking methodology that Viking performs in it's SSD test facility. The SSD performance stated in the Viking SSD datasheets can be achieved by following the same Viking approach to SSD benchmarking which has been outlined in this document.

viking TECHNOLOGY | A RF, Optical, Microelectronics and Memory Company

Table of Contents

1 INTRODUCTION 3

2 ATA SECURITY COMMAND CODES 4

3 AES-128 ENCRYPTION 4

4 AES-128 IMPLEMENTATION IN VIKING FAMILY OF ELEMENT SSD'S 5

4.1 Key Management 6
4.1.1 Standard Internal Keys 6
4.1.2 Drive-Unique Keys 6

4.2 Booting the Drive 6

4.3 Cryptographic Erase 8

5 DIAGNOSTIC MODES AND PASSWORD PROTECTION 8

5.1 Diagnostic Unlock 8

5.2 Physical Block Access and AES 8

5.3 User Keys and Drive Passwords 9

5.4 Secure Erase 9

6 AES-256 ENCRYPTION 10

7 REFERENCE DOCUMENTS 10

8 ABOUT VIKING TECHNOLOGY 10

9 REVISION HISTORY 10

Table of Figures

Figure 3-1: Key Block Cipher Symmetry of AES 4
Figure 4-1: Viking Element SSD Controller AES Block Diagram 5
Figure 4-2: Use of Keys during Boot 7

1 Introduction

The purpose of this document is to describe the AES encryption for the Viking Element family of SSD's. As baseline information, it is subject to change as AES technology improves. The document does not fully describe any industry-standard interface; for complete information on any standard, see the document that defines that standard.

All Viking Element SSD's are self-encrypting drives (SED), with a bulk data encryption feature that provides automatic hardware-based 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.

The Element SSD protects sensitive data using AES-128, AES-256, ATA Secure Erase features and TCG security enhancements for enterprise-class flash drives. The encryption attributes for 6Gbps based flash controllers are as follows:

- AES-128 in CTR mode
  - Back-end security, IP protection
  - Always on with unique key
- AES-256 engine in XTS mode
  - 4 ranges with associated different keys
  - Simultaneous access to multiple bands w/o key reloading
  - Hardware-assisted shadow MBR (Master Boot Record)
- Fuse-based OTP (One Time Programming memory) for unique master key
- Hardware non-deterministic random number generator (RNG)
- Three firmware module options
  - Deterministic random number generator (default module for SSD)
  - Signature verification
  - Digital signature verification of the download image
- FIPS-197 certification for AES-128

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

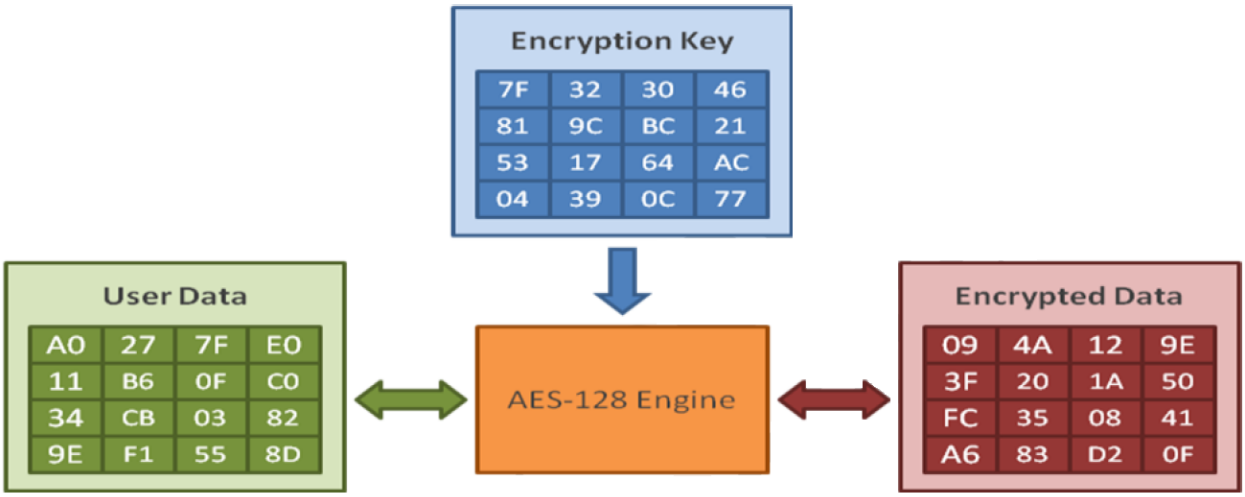
The ATA Security Mode command set for Viking SSD's consist of:

- 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 AES-128 Encryption

The Advanced Encryption Standard (AES) was developed by the National Institute of Standards and Technology becoming an official United States standard in 2002. AES is based on the Rijndael algorithm, developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. It is widely used in both hardware and software systems due to its low system resource requirements, high performance, and ease of implementation.
AES is considered a symmetrical key block cipher. The AES algorithm operates on fixed 128-bit blocks of data. As a symmetrical cipher, the same encryption key is used to encrypt and decrypt a block of data. AES supports three different key lengths. The SSD controller implements AES-128, which utilizes 128-bit encryption keys.
Within the AES engine, a series of transformations based on the encryption key and the user data are performed in order to produce encrypted data.

Figure 3-1: Key Block Cipher Symmetry of AES

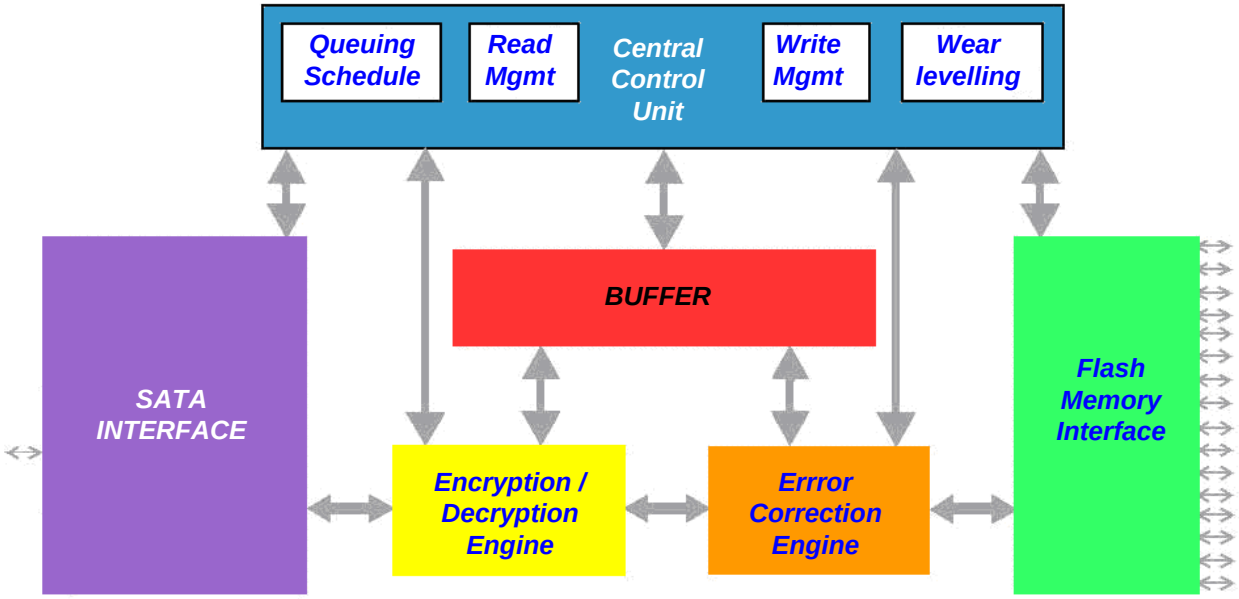


No cryptographic break has been discovered for AES. Exhaustive methods are impractical due to the number of possible keys. There are over three hundred trillion, trillion, trillion potential key values for AES-128. If one trillion key values could be tested in just one picosecond, it would take three hundred trillion years to test all possible values.

4 AES-128 Implementation in Viking family of Element SSD's

The Element SSD controller has an AES-128 engine to encrypt and decrypt all user data and metadata written to the SSD flash memory. The relationship between the ECC data correction engine and the AES engine ensures that correctable data errors do not prevent data decryption. AES encryption is an integral part of the drive datapath and cannot be disabled for normal operation. In addition to enabling a number of security features, AES encryption also randomizes data being written to flash memory, which is beneficial for reliability and overall flash memory endurance.

Figure 4-1: Viking Element SSD Controller AES Block Diagram



4.1 Key Management

4.1.1 Standard Internal Keys

All Viking SSD's are shipped with a set of two standard internal keys:
• Boot Loader Key -- Used to read the boot loader stored in flash during power-on.
• Firmware Download Key – As all Viking firmware releases are distributed in encrypted form, this internal key is used to decrypt all incoming firmware downloads.

There is no software or test mode mechanism providing external access to these two internal encryption keys.

4.1.2 Drive-Unique Keys

During the firmware download process, two random drive-unique keys are generated:

• Firmware Key: This drive-unique key protects the firmware code that resides in flash memory. It prevents unauthorized access to the firmware code. The key is stored in flash. Each time firmware code is read from flash memory, it is decrypted using this key.

The randomly generated firmware key is encrypted by and protected with the internal Boot Loader Key (described above).

• User Data Key: This drive-unique key protects all user data and meta-data. It prevents unauthorized access to user data. The key is stored in flash. Each time user data or meta-data is retrieved from flash memory, it is decrypted using this key.

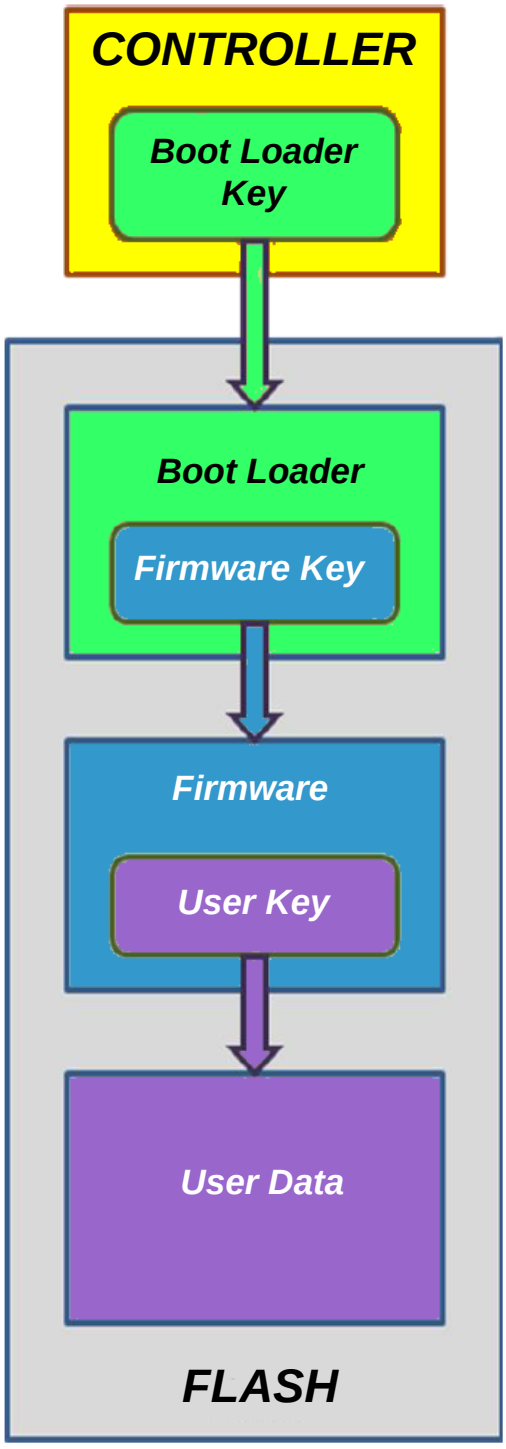
The randomly generated user data key is encrypted by and protected with the firmware key (described in the previous bullet).

After hardware reset deassertion, once the SSD boot process has completed, only the above two drive unique keys are used during normal operation.

4.2 Booting the Drive

Figure 1 illustrates the use of the Boot Loader Key, Firmware Key, and User Data Key, as well as the physical location of each of these keys.

Figure 4-2: Use of Keys during Boot



4.3 Cryptographic Erase

Changing the user data key renders all user data and meta-data previously written to the device unreadable. This is referred to as a cryptographic erase.
Because the firmware key is independent from the user data key, a cryptographic erase has no effect on the firmware resident in the flash memory. Combining a cryptographic erase with a metadata reset results in a fast, secure erase of the entire drive. The approximate strength of the cryptographic erase using Pollard Rho Method is 300 bits. Please contact Viking for more information on secure erase support.

5 Diagnostic Modes and Password Protection

The SSD controller Diagnostic Command set provides access to flash memory blocks when they are in the physical state (Please contact Viking for specifics on physical access, raw access, and block state).

5.1 Diagnostic Unlock

Diagnostic unlock commands do not involve the AES system.

5.2 Physical Block Access and AES

Read and write operations on blocks in the “physical state” do not use the User Data Key or the Firmware Key:

• Diagnostic commands “ReadPhysical” and “WritePhysical” use a separate Diagnostic Key, thus ensuring that user data is not retrievable in decipherable form when issuing these commands.

• Diagnostic commands “ReadRaw” and “WriteRaw” use no key and bypass the AES engine entirely, again ensuring that user data is not retrievable in decipherable form when issuing these commands.

In either case, any previously written user data is not decipherable as a result of a physical or raw read operation. (Physical state block erasures do lose any user data inside. Data written to a physical state block (using either Physical or Raw write commands) is not retrievable using normal non-diagnostic commands.)
Thus, data resident in a physical state block is erasable and corruptible, but not retrievable, using diagnostic commands and mechanisms.

5.3 User Keys and Drive Passwords

AES encryption/decryption is essentially a closed system between the controller and the flash memory. A Drive Password is a means of access protection between the host system and the drive. The number of password retries allowed is 5.

There are three scenarios:

1. A Drive Password has not been established. In this case, all host read accesses result in user data being decrypted at the controller's flash memory interface, and user data is then delivered to the host system in decipherable form.

2. A Drive Password has been established. The SSD controller stores a Drive Password in flash memory. It is protected by the User Data Key. For any subsequent read operations, there are three sub-cases:

a. The host system knows the correct Drive Password. It is delivered to the controller via the ATA SET PASSWORD command, at drive discovery time. The controller verifies the password's correctness and opens the drive to accesses (i.e., "security unlocked" state). All host read accesses result in user data being decrypted at the controller's flash memory interface, and user data is then delivered to the host system in decipherable form. All write data is encrypted when written and is retrievable as long as a host provides the correct drive password at discovery time to "open" the drive to access.

b. The host system does not know the correct Drive Password. The incorrect password is delivered to the controller via the ATA SET PASSWORD command, at drive discovery time. The controller responds to the SET PASSWORD command with a "command aborted" status. The drive remains security-locked.

c. The host system does not know the correct Drive Password. No password is delivered to the controller. The drive remains security-locked.

5.4 Secure Erase

All map entries and AES key(s) are zeroized upon a ATA secure erase. The recommended way to access the ATA security command set after an OS boot (e.g. hdparm or any other SW utility) is to use a Viking provided utility called Toolbox 2.0 (available February 2012). This will allow users to easily set the ATA password without directly using the ATA Security Command opcodes.

6 AES-256 ENCRYPTION

AES-256 contains a fuse block with 256 bit root of trust that is unique to each controller chip. The root file system encryption key is generated from this, in addition to other wrapped keys. The AES-128 engine has its own generated unique key using a hardware non-deterministic random number generator. This is all managed in a security firmware module on the SSD which is isolated from the core controller firmware.

7 Reference Documents

- IEEE SA - 1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
- Viking Element SSD Product Datasheets
  http://www.vikingmodular.com/products/ssd/ssd.html
- Viking Application Note
  AN0010 - Secure_Erase and Military_Purge_Routines

8 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 20 years. For more information visit http://www.vikingtechnology.com.

9 Revision History

6/8/11		Added the relative strength of cryptographic erase
12/21/11		Added a list of ATA Security Command op codes
01/09/12		Added notes and references for AES-256
09/05/17		Revise logo and address

Global Locations				
US Headquarters	Canada Office	Texas Office	India Office	Singapore Office
2950 Red Hill Ave. Costa Mesa, CA 92626 Main: +1 714 913 2200 Fax: +1 714 913 2202	500 March Road Ottawa, ON K2K 0J9 Canada	1201 W. Crosby Road Carrollton, TX 75006 USA	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

A RF, Optical, Microelectronics and Memory Company