TECHNICAL WHITE PAPER

FLASHARRAY SECURITY AND COMPLIANCE

AN OVERVIEW

PURESTORAGE®

TABLE OF CONTENTS

INTRODUCTION

There is no doubt that data security is an increasingly critical concern for organizations worldwide. Lack of effective technology and weak security policies can leave an organization open to liability. One of the drawbacks to improving security is the perceived administrative overhead associated with doing so. An organization must weigh new processes and technologies with all of the new complexity in securing and managing that data. Within the industry there is an expectation of friction between ease of administration and implementation of comprehensive data security, which can be a barrier organizations must overcome. Or, alternatively, they must find a way a better way to get the results they desire.

We at Pure Storage believe that data needs to be secured to the highest possible standards, and that this level of security should be *transparent* to customers. By transparent, we mean invisible to the customer and requiring zero management. Pure Storage® accomplishes this by securing data at rest with AES-256 bit encryption. Moreover, our data encryption occurs without impact to performance and while maintaining full data reduction capabilities. Pure Storage FlashArray encryption is FIPS 140-2 certified, NIST compliant, NIAP/Common Criteria validated, and PCI-DSS compliant. The efficacy of our data encryption and data erasure have been validated by Kroll OnTrack, one of the industry's leading security firms.

With the increase in data protection and compliance regulations required by various industries, countries and regions, the high level of built-in security and encryption capability available in a FlashArray represents an effective way to help achieve data protection regulatory compliance. To see how FlashArray can contribute to the European Union's General Data Protection Regulation, read our report, FlashArrays and GDPR Compliance.

Achieving high levels of security does not equate to product complexity – Pure Storage FlashArray encryption at rest is protected by an internal process that removes key management from users. Not only does this allow our customers to focus on data storage, it also removes human error from the process. Our key management is sophisticated, including automatic key rotation, periodic key regeneration, and unreadable partitioned keys that are spread over FlashArray flash modules. In the event of total array loss, multiple steps are required to reconstruct the data, requiring physical access to a majority of the modules of the array, access to all secure keys that are partitioned across all flash modules, and a deep understanding of the hidden logical structure of the internal databases.

To completely lock down the array, even in the event of total loss to a highly-skilled intruder with deep product-specific knowledge, Pure Storage also provides Rapid Data Locking through two optional external key technologies:

- **USB connected Spyrus Rosetta II Smartcards.** A FlashArray can be completely locked (data rendered permanently unrecoverable) with the removal of the smart card and power loss to the array
- **KMIP (Key Management Interoperability Protocol) remote key server.** A FlashArray can be locked down by revoking a remote key and powering off the FlashArray.

ABOUT DATA AT REST ENCRYPTION

The FlashArray encrypts data with the use of three dependent layers of internal keys:w an Array Key (figure 1), an SSD Key (figure 2), and a Data Encryption Key (figure 3).

The array key is generated with a random secret and then broken up over a number of SSDs. This method assures that half of the array drives, plus two more, are required to recreate the current access keys. SSD keys are never exposed on any array interface, nor does any single SSD contain a full encryption key.

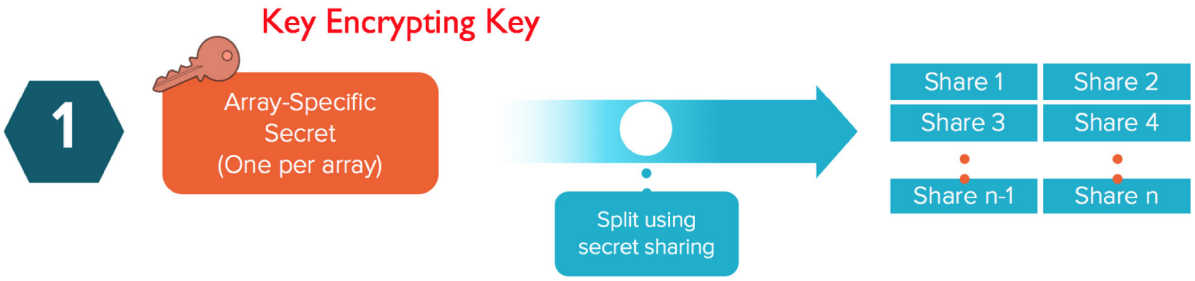

FIGURE 1. Array key generation

Array Key (key encrypting key)

- Created at array initialization
- Distributed across SSDs using “secret sharing” algorithm
- Changed every 24 hours, and when there are configuration changes

When a flash module needs to be replaced, it is inserted into the array and initialized. At this point, a device-specific access key is created and sent to the device. The FlashArray must supply the access keys to unlock any flash module – and once the device key is written to the flash module, it cannot be read back. These various flash module access keys are only accessible with the Array key.

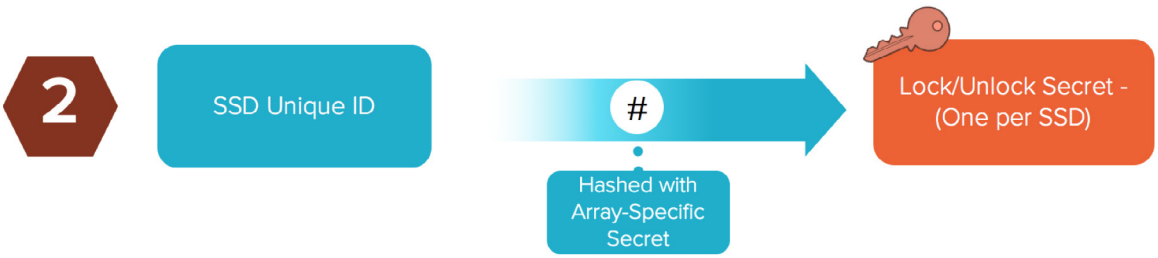

FIGURE 2. SSD access key generation

SSD Access Key (unlock key)

- Generated at boot with hash of Array Key and SSD Key
- Unique per device (NVRAM and SSD)
- Cannot not be read back

Finally, the array uses a data encryption key to encrypt data stored on flash modules. Like the SSD access key, the encryption key is also partitioned across all of the devices. An array's data encryption key is constant for the life of the array, but it is re-encrypted each time the array creates new device access keys. Like SSD access keys, array data encryption keys cannot be exposed or read back.

FIGURE 3. Data encryption key generation

Data Encryption Key

- Requires unlocked SSDs since it is stored and partitioned on the SSD itself
- Cannot be read back like the SSD Key
- Armored by Array Key using a AES256 Key wrap

The Array Key expires every 24 hours – this is required to unlock the flash modules, which have a unique ID that must match the FlashArray to device hash. Once a quorum of drives are unlocked (half of the drives plus two), only then can the Data Encrypting Key be read.

> This process runs continuously in the background, assuring that no single device, or even half of the devices, can allow data access.

RAPID DATA LOCKING (RDL)

Some environments require external key management for locking down an array that is forward deployed. We provide two solutions:

1. USB connected Smartcards
2. KMIP connectivity for remotely managed keys

Smartcard RDL

With Smartcard RDL, customer-programmable Spyrus Rosetta II Smartcards act as security tokens that enhance SSD access keys and participate in key regeneration at power-on. Once unlocked, flash modules are accessible, but when smartcards are removed from the USB connected readers, the SSDs cannot be unlocked at power-on. For example, if an array is transported separately from its smartcards, data on its SSDs cannot be read or written, even with specific Pure Storage knowledge and the required skills in cryptography. The smart cards act as a secondary SSD key, and without access to them, none of the flash modules can be unlocked.

KMIP RDL

Conceptually, KMIP RDL works the same way – a secondary user-controllable key is introduced that allows for unlocking the array's flash modules. Instead of being physically connected to the array through a USB card reader, KMIP keys are remotely accessed from a KMIP server. Without access to the server, the flash modules cannot be unlocked on power-on.

Data Encryption at Rest

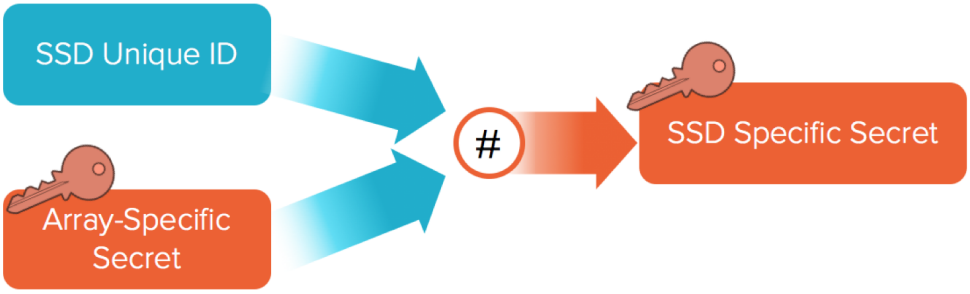

FIGURE 4. KMIP remote access

Data Encryption at Rest with Rapid Data Locking enabled (shown with both USB and KMIP RDL)

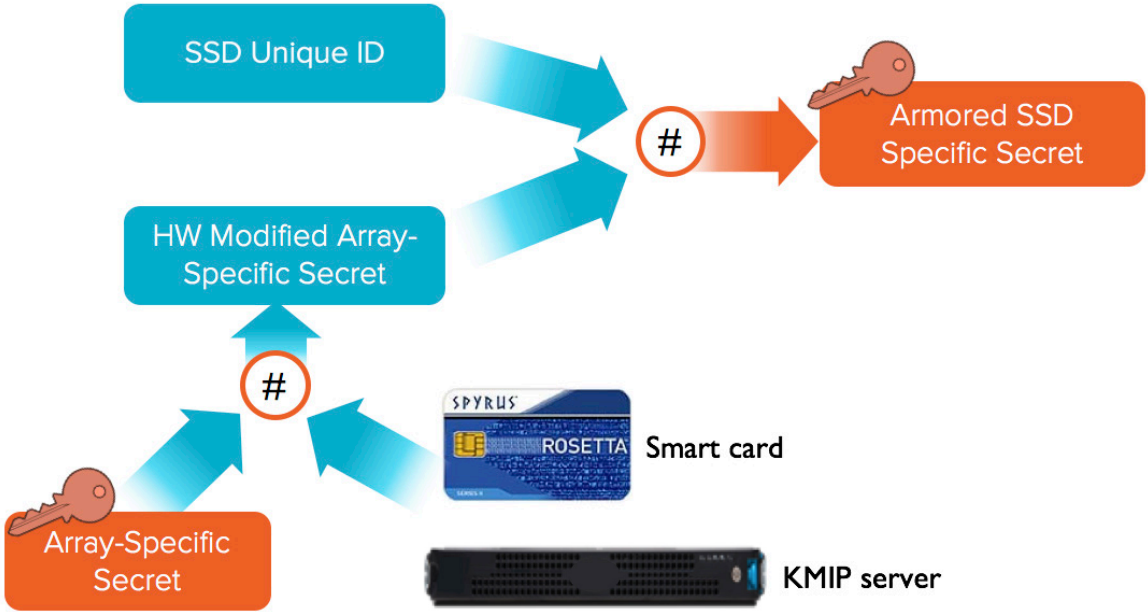

FIGURE 5. KMIP remote access with RDL

> RDL can be enabled during installation, or at any time thereafter. Once enabled, RDL is permanent. It applies to all of an array's SSDs, including those added afterward.

COMPLIANCE AND CERTIFICATION

The FlashArray is FIPS 140-2 certified, Common Criteria certified, and PCI-DSS compliant. The following are the NIST validations for the algorithms used for encryption.

AES [FIPS 197 and SP 800-38A]

AES: http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html Validation nr. 3181

[FIPS 198-1]

HMAC: http://csrc.nist.gov/groups/STM/cavp/documents/mac/hmacval.html Validation nr. 2007

[FIPS 180-4]

SHS: http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm Validation nr. 2633

[FIPS 140-2 Certification]

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2467

NIAP Certification (with Purity 4.7+)

https://www.niap-ccevs.org/st/Compliant.cfm?pid=10664

Common Criteria (CC) Information

The Common Criteria Recognition Arrangement (CCRA) is an international agreement that defines criteria for specifying and evaluating security in information technology products.

Strict CC compliance requires certain Pure Storage FlashArray capabilities – for example, PhoneHome and RemoteAssist – be restricted. These features can be enabled, but full relaxation of Common Criteria compliance would require Technical Support engagement.

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is a standard for managing credit card information of customers. It defines rules of security for various data center devices.

PCI-DSS specifies a number of requirements which are met or exceeded by criteria in the Pure FlashArray Common Criteria certification. Please see the table on the next page.

PCI DSS REQUIREMENTS	PURE STORAGE FLASHARRAY SOLUTION
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	The drive encryption is not tied to any user account. The data encrypting keys are different from the keys used to unlock/lock the drives and they never leave the system.
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	Encryption or drive lock/unlock keys never leave the system and hence no one can have access to the keys.
3.6.1 Generation of strong cryptographic keys	Encryption Algorithms used by the FlashArray are FIPS certified: • AES [FIPS 197 and SP 800-38A] • [FIPS 198-1] • HMAC: http://csrc.nist.gov/groups/STM/cavp/documents/ mac/hmacval.html Validation nr. 2007 • [FIPS 180-4] • SHA: http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm Validaton nr. 2633
3.6.2 Secure cryptographic key distribution	Encryption keys are stored in their respective interface and not accessible externally.
3.6.3 Secure cryptographic key storage	All keys are encrypted and distributed over SSDs using secret sharing algorithm
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod	SSD keys change automatically every 24 hours or with any change in SSD configuration; replacements, upgrades, etc.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	Keys are encrypted within the SSDs and then partitioned across half of all SSDs plus two. Compromise would require access to many SSDs to re-generate the Array key. Keys are also stored in DRAM, and are lost when the array is powered off. Accessing keys in DRAM would require live access to the array without loss of power.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.	No clear text keys exist in a Pure Storage FlashArray.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	Rekeying operations are internal to the system and there are no external unauthorized keys used for encryption or locking/unlocking SSDs

SUMMARY

Pure Storage, with a continuous emphasis on simplicity, has implemented rigorous security measures including AES-256 bit encryption, data erasure, rapid data locking technologies, key management, and a robust encrypt/decrypt process. These features meet or exceed internationally recognized security standards such as FIPS 140-2, NIAP/Common Criteria and PCI-DSS. Coupled with comprehensive organizational security measures, FlashArray can help customers meet security requirements and data compliance regulations around the world – including the recently updated GDPR. We have achieved this without compromise in product serviceability, performance, or our industry-leading data reduction capabilities.

ps_wp9p_purity-secure_ltr_01