Aug
2015

Trusted Computing Group and NVM Express Joint White Paper: TCG Storage, Opal, and NVMe

In this paper…

- Describes how TCG-based security solutions are an excellent fit for NVMe storage solutions, from enterprise to client.
- TCG Storage and Opal SSC background, and comparisons of Opal SSC to legacy management interfaces.

Trusted Computing Group

3855 SW 153rd Drive
Beaverton, OR 97003

Tel (503) 619-0562
Fax (503) 644-6708

admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Copyright © 2004 – 2015 Trusted Computing Group®
(www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc.
(www.nvmexpress.org.) All Rights Reserved

TRUSTED COMPUTING GROUP

Trusted Computing Group and NVMe Work Group Joint White Paper: TCG Storage, Opal, and NVMe

INTRODUCTION

The Opal "Family" of specifications published by the Trusted Computing Group provides a scalable infrastructure for managing encryption of user data in a Storage Device, as well as extensibility to enable features beyond "data at rest protection".

The protocols associated with management of encryption capabilities provided by Opal and its subset specs, Opalite and Pyrite, range from light to thorough, with further scalability up to meet even fuller featured levels of capability; and further scaling down possible to enable even more use cases than those already being addressed.

Opalite and Pyrite were designed for equivalency to the ATA Security Feature Set, while remaining scalable to the future and using a protocol in common with Opal. However, even Opal is simple for host applications to configure for basic use cases, such that an application that can manage an implementation of Opalite or Pyrite could also manage an implementation of Opal.

The scalability of the architecture and solutions embodied in the TCG Storage specifications provides an ideal match for the scalability provided by the NVMe specification and aligns with the Opal Family of specifications as the security management interface for both NVMe client and data center Storage Devices.

The following sections describe the Trusted Computing Group Storage Work Group; the Opal, Opalite, and Pyrite specifications for managing encryption of user data; drawbacks of alternatives to the Opal family of specs; and the areas where NVMe Work Group and TCG Work Group can collaborate to provide enhanced solutions that combine the benefits of the two specifications.

TCG STORAGE

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open, vendor-neutral, global industry standards. One of the TCG's work groups is the Storage Work Group (SWG).

The SWG has defined and published a number of specifications. These specifications define architecture for Storage Device-based security features, which are designed to be configurable and manageable under policy-based access control. This means that the capabilities of the Storage Device are able to be configured to conform to the security policies of the trusted platform or associated organization.

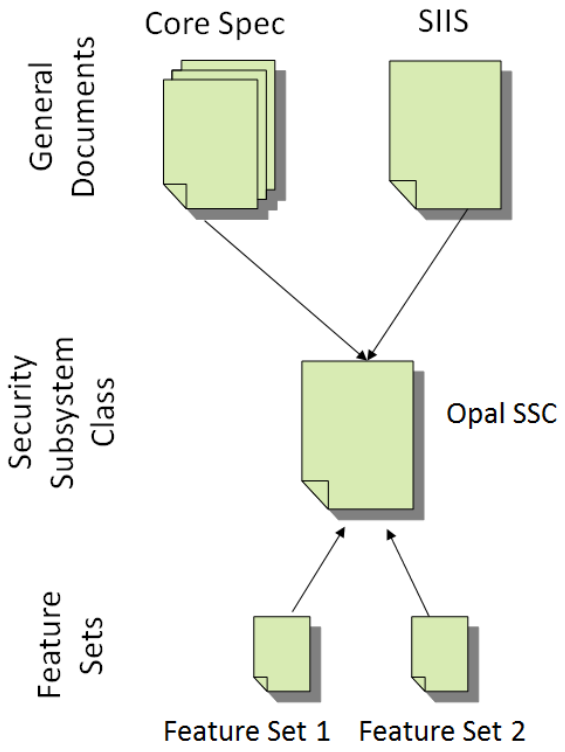
The primary TCG SWG specification is the "TCG Storage Architecture Core Specification", or "Core Spec." This document defines in detail the components that can be implemented by a Storage Device to provide various features. The Core Spec defines a storage interface-independent communications protocol used by host applications to manage features, as well as the data structures and commands associated with a variety of other capabilities.

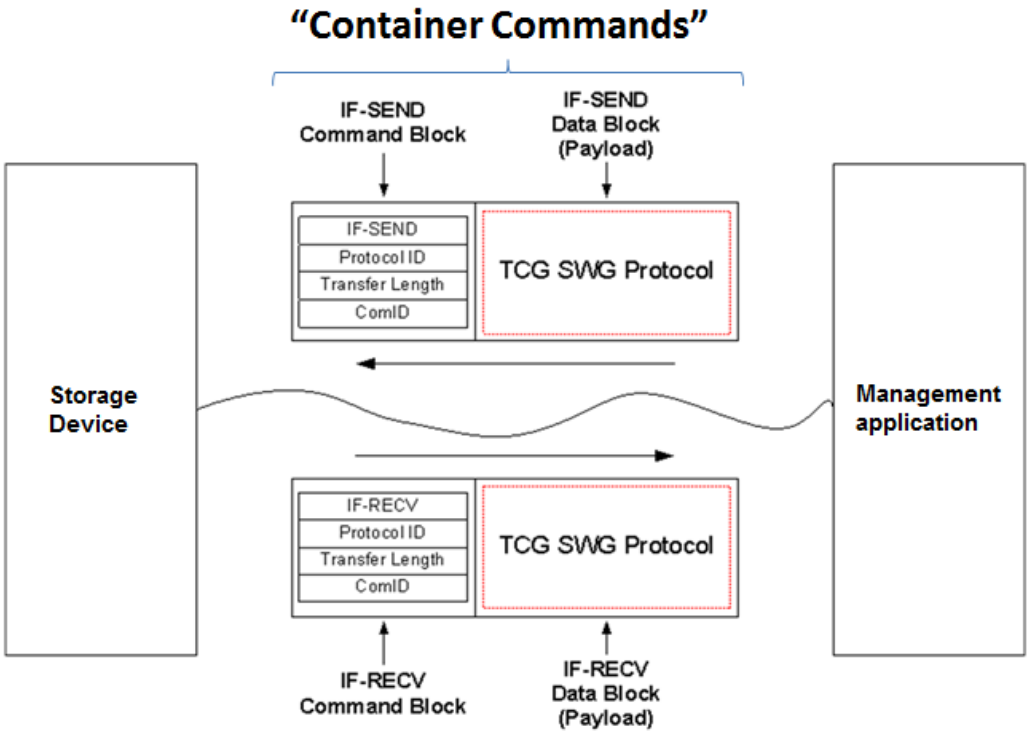
Copyright © 2004 – 2015 Trusted Computing Group® (www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc. (www.nvmexpress.org.) All Rights Reserved

Because of the usage of container commands, and due to the fact that some TCG Storage capabilities have effects on the Storage Device and its life cycle, the SWG has defined a “glue” spec, called the “TCG Storage Interface Interactions Specification,” or “SIIS”. The SIIS defines mappings to the interface container commands; includes error mappings from errors defined in TCG Storage specs to relevant errors in the underlying interface specifications; and mappings from TCG Storage-defined reset events to reset events defined for the underlying interfaces.

One set of capabilities defined in the Core Spec includes mechanisms for managing access control to user data stored on the Storage Device, including controlling Media Encryption, Key Management, and Read/Write Lock State. The “TCG Storage Security Subsystem Class: Opal”, also called “Opal SSC” or just “Opal”, is an implementation profile for Storage Devices that incorporate this functionality.





Copyright © 2004 – 2015 Trusted Computing Group®
(www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc.
(www.nvmexpress.org.) All Rights Reserved

Storage Devices that implement Opal are built to protect the confidentiality of stored user "Data at Rest" (DAR) against unauthorized access once it leaves the owner's control, when or after the Storage Device has been power cycled.

Use Cases that can be performed using the management interface defined in the Opal SSC include activation and provisioning of the locking and encryption management capabilities; locking and unlocking LBAs by the host; pre-boot authentication; and repurpose/end of life of the Storage Device.

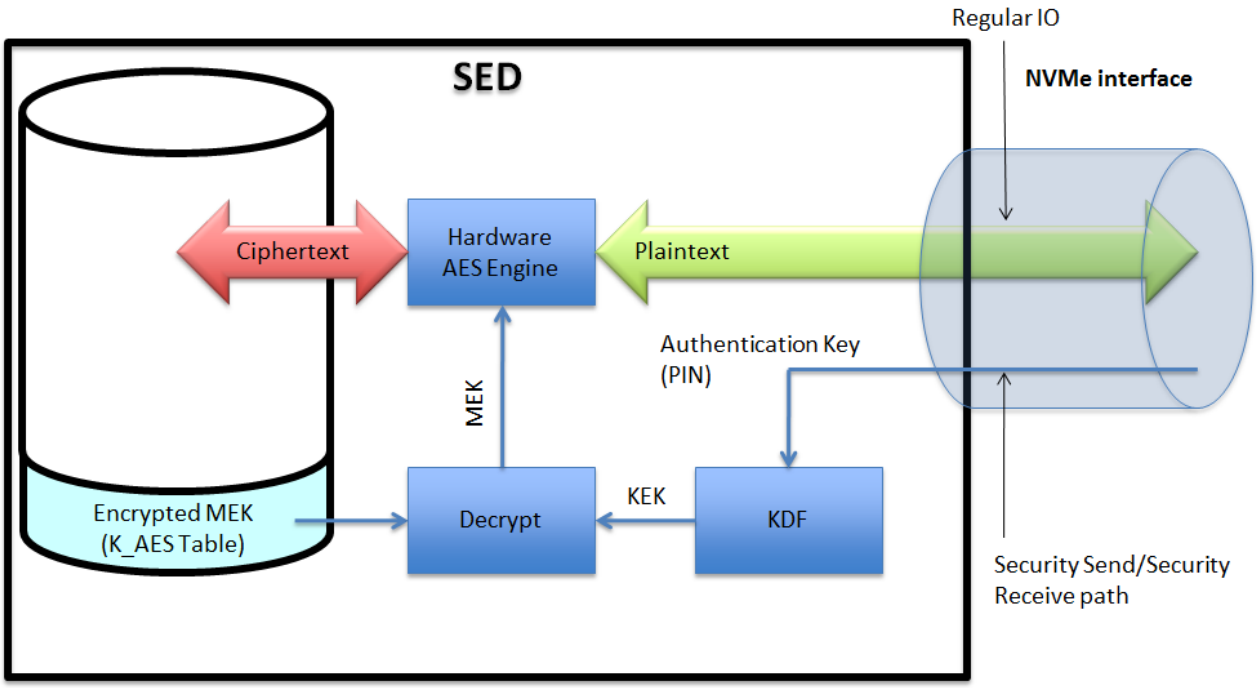
Self-Encrypting Drive Basics

A Self-Encrypting Drive (SED) is a Storage Device that integrates encryption of user data at rest. All user data written to the Storage Device is encrypted by specialized hardware implemented inside the Storage Device controller. The data is decrypted as it is read. The encryption and decryption are performed using a Media Encryption Key (MEK) generated internally in the Storage Device.

Opal SSC defines a management interface for a host application to activate, provision, and manage encryption of user data. The specification includes data structures and their required content, and mechanisms for managing and configuring Authentication Credentials and access controls.

Opal SSC provides a mechanism by which an Authentication Credential (i.e. a password) can be set by a host application that manages the Opal SSC functionality in the Storage Device, in order to enable control of access to the User Data via "Locking".

When an Authentication Credential has been set and the device is locked, it is not possible to access User Data. Once the correct Authentication Credential has been supplied to the Storage Device by the host, and the Storage Device is unlocked, data can be read from and written to the device.



Copyright © 2004 – 2015 Trusted Computing Group®
(www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc.
(www.nvmexpress.org.) All Rights Reserved

The Authentication Credential is a value derived from the user's password/passphrase, or some other authentication mechanism. Opal SSC is agnostic to the mechanisms used to capture such an authentication value from the user.

When implemented properly, the operation of setting an Authentication Credential enables "Cryptographic Protection of Data at Rest". The Storage Device uses a value derived from the Authentication Credential as a "Key Encryption Key", or KEK. Once the Authentication Credential is set, the KEK is used to encrypt the MEK prior to MEK's storage on media. The MEK is only stored persistently in encrypted form. Any instances of a plaintext MEK are only held internally to the Storage Device controller, and only temporarily while the Storage Device has power. When the Storage Device loses power, the plaintext MEK is lost.

After a Storage Device power cycle, since the plaintext MEK has been "forgotten" by the Storage Device, it is no longer possible to read or write data via the storage interface. The Storage Device is "locked". In order to gain access to user data in plaintext, it is necessary for the user to supply the correct unlock password/passphrase. The host application accepts a password as input from the user, generates an Authentication Credential from the supplied password, and sends the Authentication Credential to the Storage Device to attempt to unlock access to the data.

If the supplied Authentication Credential is correct, the Opal firmware in the Storage Device will be able to successfully decrypt the encrypted MEK, which can be used to encrypt/decrypt data. If the Authentication Credential is incorrect, the Opal firmware will not be able to successfully decrypt the encrypted MEK, and data will remain inaccessible.

Opal SSC

Opal SSC provides an interface that allows a host application to manage features related to user authentication and media encryption. Because the framework architecture on which Opal SSC is built (as defined in the Core Spec) is easily extensible, new features can be added to address additional use cases.

Opal SSC provides a full featured device implementation profile, with a variety of features that can be taken advantage of through Opal management software.
This specification defines a variety of features.

- Opal SSC defines a requirement to support encryption of user data, using either AES-128 or AES-256.
- Hardware-based encryption of user data can be scaled to meet bandwidth capabilities of the Storage Device.
- An Admin credential is used to perform provisioning and configuration.
- Multiple User credentials are supported, and can be assigned to perform various actions within the Opal subsystem.
- The Storage Device can be subdivided into multiple "Locking Ranges". Each of these is a range of contiguous LBAs.
- Each Locking Range is encrypted with a different Media Encryption Key.
- Each Locking Range can be unlocked independently of the others.
- Zero or more Users can be assigned permission to unlock Locking Ranges.
- Each Locking Range can be cryptographically erased independently of the others. Cryptographic erase is a process by which a MEK is destroyed, and a new MEK is generated. Eradication of a MEK means that the data which that MEK was used to encrypt is no longer able to be decrypted

Copyright © 2004 – 2015 Trusted Computing Group® (www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc. (www.nvmexpress.org.) All Rights Reserved

- Zero or more Users can be assigned to cryptographically erase Locking Ranges. This provides a fast, secure way to perform repurpose or end of life operations.
- Opal supports MBR Shadowing, through which a host application can store and execute a “Pre-Boot Authentication Environment”. Such a mechanism is necessary to allow unlock of the range in which the OS is stored, in order to allow the OS to boot.

Because Opal SSC SEDs are typically thought of as “enterprise” class (i.e., corporate client) solutions, the NVMe work group made a request to the TCG Storage Work Group to consider defining a subset of the Opal SSC. Such a subset would provide a basis for SED management to a broader range of Storage Devices and platforms, including those targeted for “consumer” solutions. In response, the TCG SWG defined 2 new SSCs, “Opalite SSC” and “Pyrite SSC.

Opal Device Layout

	Size:	Area:	
Device	varies	System (firmware, TCG tables, etc.)	Access with IF-SEND and IF-RECEIVE
	128mb+	Shadow MBR Region	Typically contains pre-boot authentication app
	1k+	DataStore	Typically contains pre-boot variables
User (LBA 0 to LBA [Max])	varies	Global Range	Default range, contains user data
	Varies, set by admin	Range 1	Admin-configured range, contains user data
	Varies, set by admin	Range 2	Admin-configured range, contains user data
	varies	Global Range, Continued	(rest of the default range that is not used by any admin-configured LBA ranges)

Copyright © 2004 – 2015 Trusted Computing Group® (www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc. (www.nvmexpress.org.) All Rights Reserved

Opalite SSC and Pyrite SSC

In response to a request from the NVMe work group, the TCG SWG is working to finalize two new SSC specifications: Opalite SSC and Pyrite SSC. These two specifications are a subset of the Opal SSC.

The primary difference between Opal SSC and Opalite SSC is that Opalite defines only a single, "Global" Locking Range, whereas Opal requires support for several configurable Locking Ranges. In addition, Opalite limits the number of supported Users to 2.

Pyrite is almost identical to Opalite, with one primary difference: Pyrite does not specify capabilities for cryptographic protection of data at rest. As such, references to and support for capabilities related to encryption, cryptographic erase, etc. are absent from Pyrite.

Opalite and Pyrite provide Storage Device vendors the ability to provide different levels of solution, depending on market need, internal roadmaps, and other business and technical considerations.

Feature	Opal V2.00 SSC	Opalite SSC (Opal 2.00 subset)	Pyrite SSC (Non-encrypting version of Opalite)
Core Spec Version Supported	V2.00	V2.00	V2.00
Activation and Life Cycle	Yes	Yes	Yes
Number of Admins/Users	4 Admin, 8 User	1 Admin, 2 User	1 Admin, 2 User
Min Number of Required LBA Ranges	Global Range + 8	Global Range only	Global Range only
Min DataStore Size (General Purpose Storage)	10MB	128KB	128KB
Min MBR Table Size	128MB	128MB	128MB (Optional)
Configurable Access Control	Yes	Yes	Yes
PSID	Optional (Required in v2.01)	Required	Not Required (recommended as Prohibited due to lack of integrated data sanitization)
Media Encryption	Required	Required	Not Specified
Crypto Erase	Revert, RevertSP, GenKey methods for device and locking range level erase granularity	Revert, RevertSP, GenKey methods for device and locking range level erase granularity	No user data erase supported – relies on native interface erase capability

Copyright © 2004 – 2015 Trusted Computing Group® (www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc. (www.nvmexpress.org.) All Rights Reserved

Other than these differences, the Opal, Opalite, and Pyrite SSCs are very similar. They all rely on the same communications protocol, on a common set of data structures, and on a common set of commands. Because the management interface is common, it is straightforward to design and implement software to manage Storage Devices based on the Opal Family.

ATA Security

"ATA Security Feature Set", or ATA Security, defined by INCITS T13, is commonly referred to as the "Hard Drive Password". The ATA Security Feature Set has been in existence and deployment for years. The ATA Security Feature Set is deployed on the majority of modern ATA-based (including SATA) drives, and is managed (and manageable) by BIOS/platform firmware.

ATA Security (like Opal and its subset SSCs) is designed with a "first comer" ownership model. The first application to set the ATA Security password, and thus "Enabling" the feature, gets ownership. ATA Security defines a Freeze Lock command, which helps control this by limiting the ability to take ownership to any entity that can execute the appropriate command sequence prior to execution of the Freeze Lock command.

Once a password has been set to enable security, and after the appropriate command is issued to authenticate a password and unlock the Storage Device, security commands can still be executed without having to supply the password again. This means that once the managing host application issues the appropriate unlock command, the command to modify the password or the command to erase the Storage Device could be issued by any entity, since the command does not need to include the password.

Capability	ATA Security	Opal
Simple access control using a User password	✓	✓
Specified to require industry grade AES cipher for data-at-rest protection	✗	✓
Remote management	✗	✓
Extensibility to other security usage models	✗	✓
Specified support for Crypto Erase	✗	✓
"Purge" level erase as specified by NIST SP 800-88	✗	✓

Copyright © 2004 – 2015 Trusted Computing Group® (www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc. (www.nvmexpress.org.) All Rights Reserved

The Freeze Lock command is used to provide control over host execution of ATA Security Feature Set commands. The managing application (typically BIOS) queries the user for their password, and transmits the password along with the unlock command in order to unlock the Storage Device. Once this occurs, the Freeze Lock command is issued in order to prevent any additional security commands from being executed unexpectedly. If Freeze Lock is not issued, then the command to change the password or erase the drive could be issued, without having to know or re-submit the user password.

Reliance on the Freeze Lock command to control access means that BIOS is the only entity that can perform management using this security interface. BIOS issues Freeze Lock, after which, by design, as long as the Freeze Lock is in effect there is no further means to perform security management. There is no inherent ability to include OS-level management components, thus limiting the ability to deploy this as a Storage Device security mechanism in environments such as enterprise/corporate clients. The corporate IT environment typically relies on OS-resident components to interact with back end management and configuration services. This also makes integration of security enhancements or new capabilities challenging.

The ATA Security Feature Set is defined as an access control mechanism only. There is no specified linkage of ATA Security to media encryption. While many vendors have deployed proprietary mechanisms that link ATA Security and media encryption, challenges with properly defining key protection schemes based on the ATA Security Feature Set raise the likelihood of propagating poor data at rest protection implementations. These proprietary linkages between ATA Security and media encryption also introduce challenges when integrating ATA Security with TCG-based capabilities like Opal.

Partly due to the lack of integration of ATA Security with requirements for media encryption, and partly due to ATA Security's antiquated definition of data erase functions as they related to modern media types (like NAND), the NIST Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization", defines ATA Security's Erase command as a "Clear" level sanitization mechanism. This is the lowest level of capability specified by the Guidelines, functionally equivalent to using IO commands to overwrite accessible LBAs. This level of data sanitization is limited in scope and applicability without vendor unique extension; is interruptible by power events and does not resume automatically; and is only available prior to execution of the Freeze Lock command.

Enterprise SSC and Data Center

"TCG Storage Security Subsystem Class: Enterprise", sometimes called "Enterprise SSC", "ESSC", or just "Enterprise", is a SSC defined by the TCG that is targeted at classic SCSI/SAS data center Storage Devices. This specification and the version 1.00 of Opal SSC were published in approximately the same time frame. However, there are significant differences between the two specifications, not the least of which is that because Enterprise SSC was designed based on a draft revision of the Core Spec, the two specs are not protocol compatible; and that the two specifications targeted different use cases.

Enterprise SSC was designed with basic data center scenarios in mind. As such, Enterprise SSC is defined in a manner that is static, and the specification supports only limited configurability, primarily to support SCSI/SAS-based Storage Devices in environments where a RAID controller has little time or capability to perform complicated configurations. This also serves to reduce testing and qualification time for the simple usage models supported.

Copyright © 2004 – 2015 Trusted Computing Group®
(www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc.
(www.nvmexpress.org.) All Rights Reserved

Feature	Opal V2.00 SSC	Opalite SSC (Opal 2.00 subset)	Pyrite SSC (Non-encrypting version of Opalite)	Enterprise SSC
Core Spec Version Supported	V2.00	V2.00	V2.00	V1.00 r0.9 (DRAFT)
Activation and Life Cycle	Yes	Yes	Yes	No
Number of Admins/Users	4 Admin, 8 User	1 Admin, 2 User	1 Admin, 2 User	1 “Bandmaster”, 1 “Erasemaster” (No Admin supported)
Min Number of Required LBA Ranges	Global Range + 8	Global Range only	Global Range only	Global Range only
Min DataStore Size (General Purpose Storage)	10MB	1MB	1MB	1KB
Min MBR Table Size	128MB	128MB	128MB (Optional)	0 MB (no pre-boot authentication support)
Configurable Access Control	Yes	Yes	Yes	No
PSID	Optional (Required in v2.01)	Required	Not Required (recommended as Prohibited due to lack of integrated data sanitization)	Not Supported
Media Encryption	Required	Required	Not Specified	Required
Crypto Erase	Revert, RevertSP, GenKey methods for device and locking range level erase granularity	Revert, RevertSP, GenKey methods for device and locking range level erase granularity	No user data erase supported – relies on native interface erase capability	Erase method

Copyright © 2004 – 2015 Trusted Computing Group®
(www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc.
(www.nvmexpress.org.) All Rights Reserved

Enterprise SSC-based Storage Devices continue to fulfill SCSI/SAS data center requirements for cryptographic protection of data at rest.

Client environments impose additional requirements beyond those satisfied by Enterprise SSC. Opal SEDs can be managed by software applications from a wide variety of software vendors, providing configurability, a life cycle management capability, and an MBR Shadowing component for pre-boot authentication, which are not supported by Enterprise SSC.

However, Opal's configurability can be transferred to data center environments, particularly given the variety of possible usages and form factors for NVMe devices (unlike Storage Devices based on other interfaces, form factors and use cases do not easily align in NVMe); and implementations of Opal that incorporate the optional "TCG Storage Opal Feature Set: Single User Mode" can be provisioned to closely emulate characteristics of Enterprise SSC's access control model in a fashion that also takes advantage of the other benefits of Opal (life cycle management, Administrator credential, etc.), providing a more scalable, future-looking set of solutions that is still able to support more limited use cases.

Summary

Opal, Opalite, and Pyrite, the Opal "Family" of specifications, provide an established means of enabling security functionality for NVMe, scalable across market segments and form factors. This is why Opal is an excellent security framework for NVMe.

Summary of Opal benefits to NVMe

- Avoids the need to add security to NVM Express standard, or rely on proprietary functionality
- Leverages the existing storage security industry standard for a consistent set of requirements
- Commonly associated features enable a more consistent and secure overall solution
- Simplifies ecosystem enabling, validation, product identification, SKU management
- Reduces standardization to a more streamlined process
- Provides an extensible interface for additional value-adds to Opal/Opalite/Pyrite functionality, as well as other storage security features

References

- Trusted Computing Group, http://www.trustedcomputinggroup.org/
- NVM Express, http://nvmexpress.org/
- TCG Data Security Architect's Guide, https://www.trustedcomputinggroup.org/resources/tcg_data_security_architects_guide
- TCG Storage Specifications, https://www.trustedcomputinggroup.org/developers/storage
- NIST Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization", http://csrc.nist.gov/publications/PubsSPs.html

Copyright © 2004 – 2015 Trusted Computing Group® (www.trustedcomputinggroup.org.) All Rights Reserved

© Copyright 2007 - 2015 NVM Express, Inc. (www.nvmexpress.org.) All Rights Reserved