SDC
STORAGE DEVELOPER CONFERENCE
SNIA SANTA CLARA, 2016

Storage Security Evolution and Advancements in NVMe* Interactions

Dr. Jorge Campello, Western Digital Corporation
Thomas Bowen, Intel Corporation

Objectives

- Overview of Trusted Computing Group (TCG*) Storage Work Group (SWG)
- Discuss current state of Opal Certification program
- Discuss work to align with NVMe*

*Other names and brands may be claimed as the property of others.

Trusted Computing Group

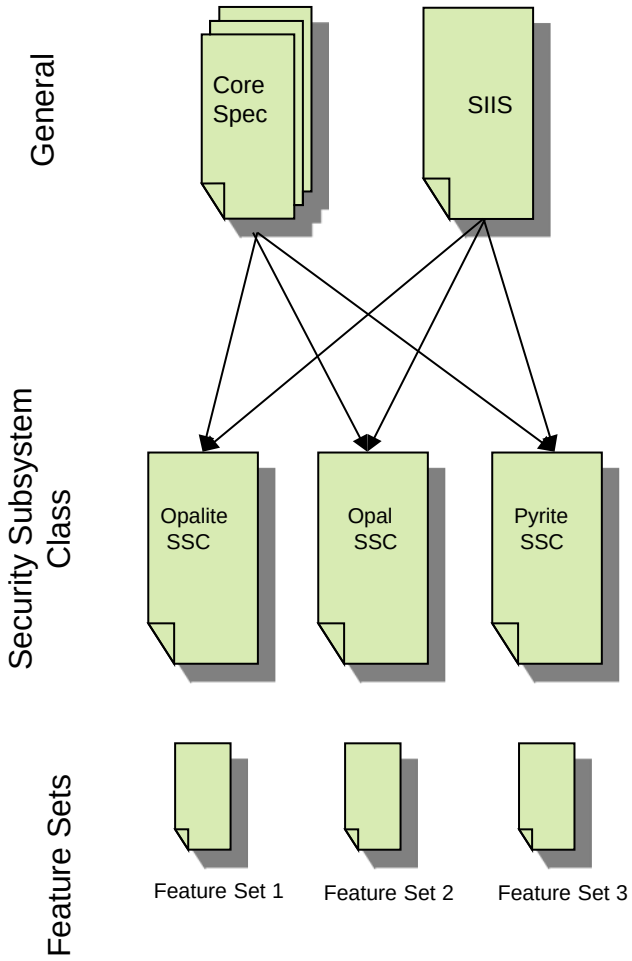
- Trusted Computing Group* (TCG)
  - Cross-industry organization formed to develop, define, and promote standards
    - Work Groups focused on TPM, Storage, Networking, Mobile, and more
  - TCG Storage Work Group
    - Defines specifications related to Storage Device-based security features

www.trustedcomputinggroup.org

*Other names and brands may be claimed as the property of others.

TCG* Storage Specifications

- **Core Specification (Core Spec)**
  - Overall architecture – a description of the underlying constructs to be used in the device specifications.
- **Storage Interface Interactions Specification (SIIS)**
  - Describes the interactions of the TCG* SWG specifications with the underlying storage interface protocols, such as ATA*, SCSI*, USB*, etc.
- **Security Subsystem Class (SSC)**
  - Device specifications, consist primarily of a subset of the functionality contained in the Core Spec.
  - Opal, Opalite, Pyrite and Enterprise
- **Feature Sets**
  - These are documents that define extensions to the basic functionality of SSCs.
    - Created to allow for simple extensions to be added to the SSC at a faster pace.
    - Additionally, it allows for features that only appeal to a subset of the market to be standardized.
    - Generally “Optional”, may be “Mandatory” by spec (e.g., PSID)



TCG Storage Specifications can be downloaded here:
http://www.trustedcomputinggroup.org/developers/storage

*Other names and brands may be claimed as the property of others.

Goals of the Storage Working Group

- Expand current use cases
  - Opalite SSC, Pyrite SSC
- Enhance ease of deployment and assurance
  - NVMe*/Namespace interactions
  - TCG* Storage Opal Test Cases, Collaborative Protection Profile
- Introduce new features based on IT, OEM, IHV, ISV pain points
  - Secure Messaging, PSID
- Expand Opal Threat Model

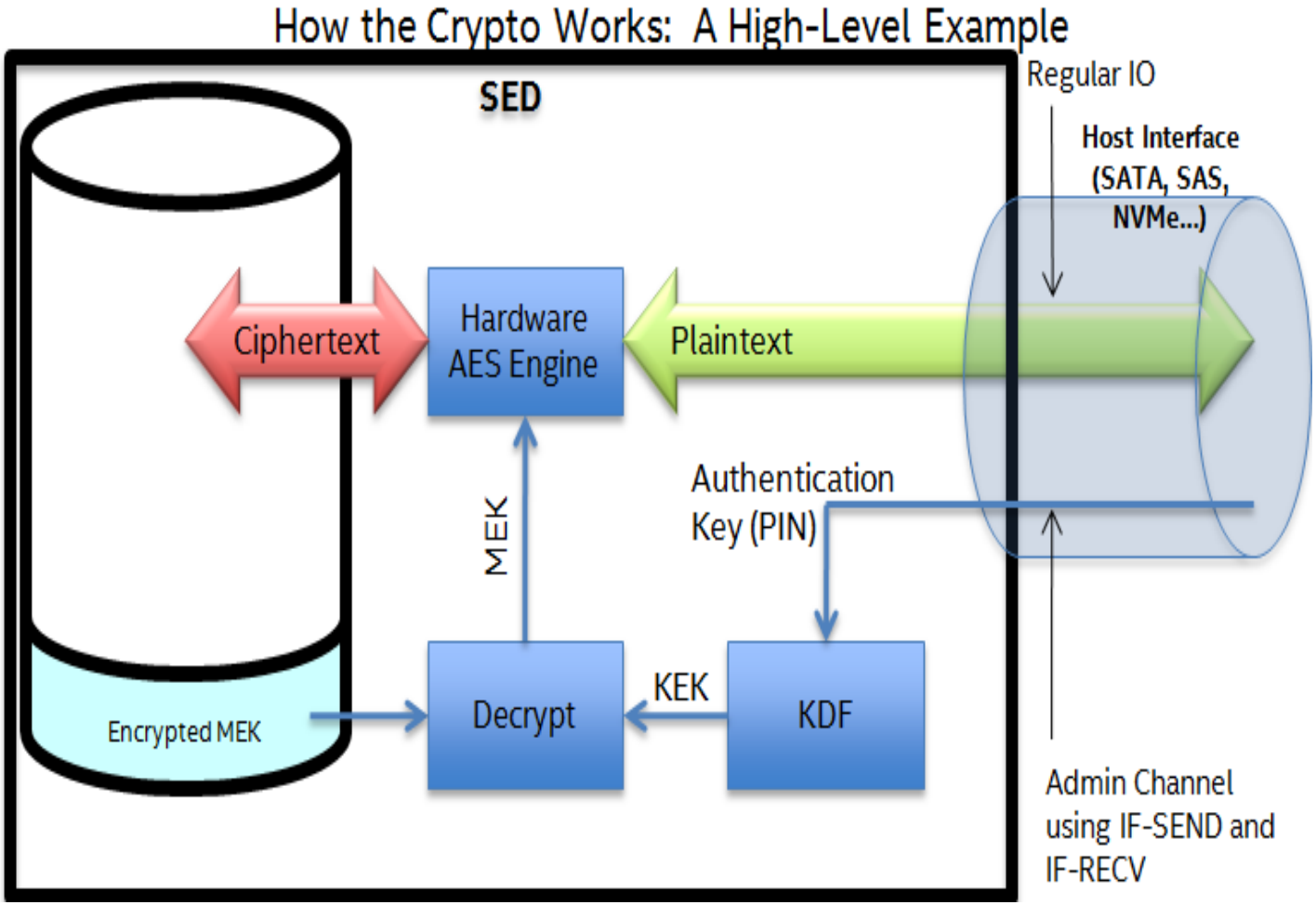
*Other names and brands may be claimed as the property of others.

Opal SSC

- Opal SSC:
  - Defines the full-featured interface for managing security features in a storage device, including device encryption.
  - **Threat model: protect confidentiality of stored user data against unauthorized access once it leaves the owner's control**
    - **Drive powered off and user has been de-authenticated from system**

- Primary Features:
  - Supports division of Storage Device user data space into multiple "LBA Locking Ranges"
  - Each LBA Locking Range has its own media encryption key.
  - Locking Ranges are locked after a storage device power cycle.
  - Admin assigns access to unlock Ranges to 0 or more Users.
  - Each Locking Range can be independently cryptographically erased.
  - The Shadow MBR region stores ISV SW "Pre Boot Environment" to capture unlock password and unlock Ranges to allow OS boot.

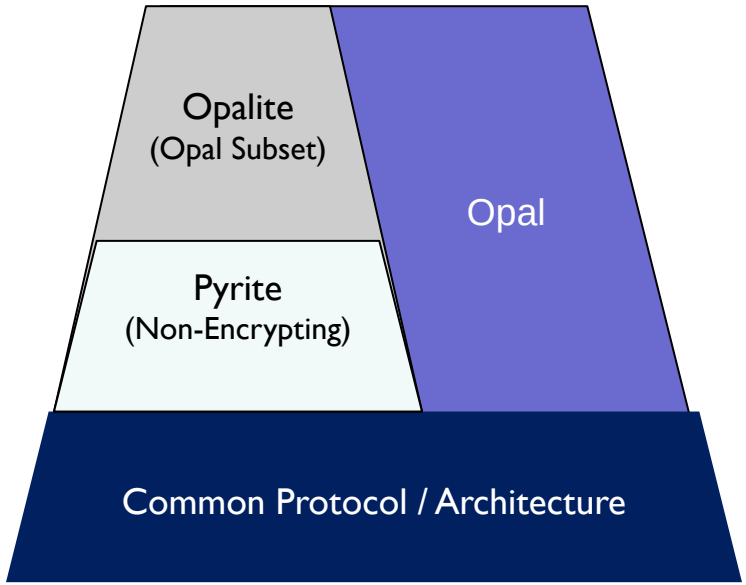
Self-Encrypting Drive (SED)



Opalite SSC and Pyrite SSC

- NVMe*'s strategy: align on Opal SSC-based solutions for security management
  - Scale across the needs of NVMe* in different Client and Enterprise (data center) solutions
- TCG* has developed a "family" of specifications to scale across the needs of NVMe* in different Client and Enterprise solutions.
- tianocore EDK2 UEFI project now supports simple password management via Opal "Family"

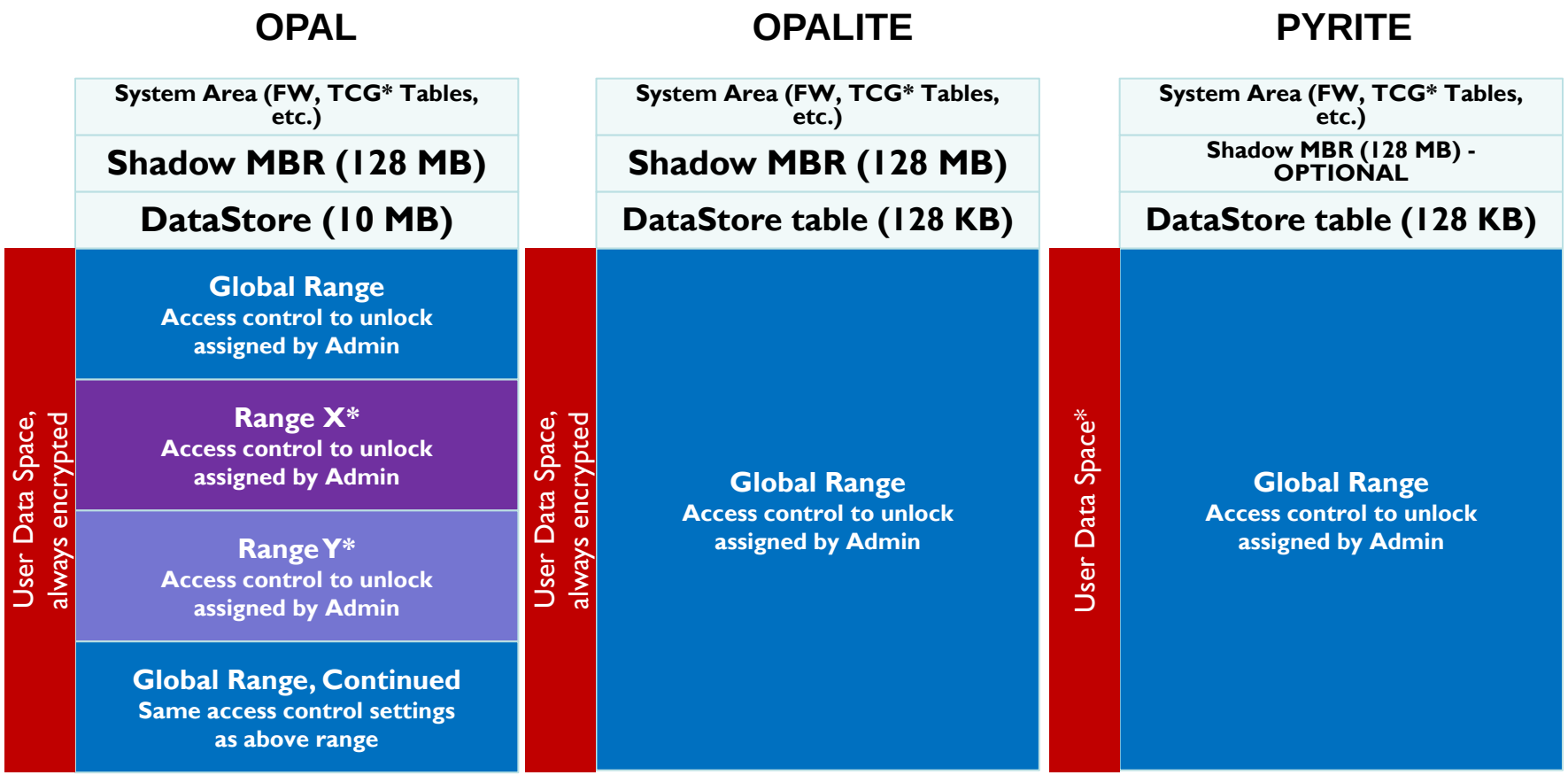
Opal "Family"



Consumers, Enterprise Client Users, and Data Centers are able to take advantage of Encryption via Opal "Family" on NVMe using the same, standardized interface

*Other names and brands may be claimed as the property of others.

Opal, Opalite and Pyrite Comparison



*Opal 2.00 supports Global Range plus at least 8 configurable ranges

*Pyrite SSC does not specify encryption of user data

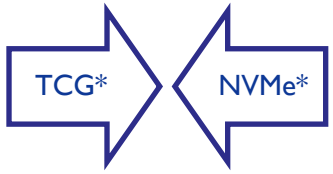
*Other names and brands may be claimed as the property of others.

Opal Compliance and Assurance

- Opal SSC Test Cases Specification
  - Baseline for Opal Certification
    - Covers Opal 1.00, 2.00, and 2.01
  - Published March 2016
- Compliance Workshop & Plugfest: May 2016
- Common Criteria Encryption Engine and Authorization Acquisition cPPs (Feb 2015)
  - Specifies security evaluation for Self-Encrypting Drives (SED) and SED management software

Opal compliance and assurance are high priority OEM/customer requests.

Namespace Interactions: SIIS v1.05+



- TCG* Storage Interface Interactions
  - Updates to Namespace Interactions in progress (targets SIIS v1.05)
- Specifies required support for 2 scenarios:
  - Multiple namespaces can be supported with all mapped to the Opal Global Range
  - A single namespace can be supported with multiple Opal "Locking ranges" all mapped within the 1 namespace

Multiple Namespaces

Opalite	
Range	Namespace
Global	NS1
	NS2
	...NSN
Pyrite	
Range	Namespace
Global	NS1
	NS2
	...NSN
Opal	
Range	Namespace
Global	NS1
	NS2
	...NSN
Range1	"Blocked"
Range2	"Blocked"
Range3	"Blocked"
Range4	"Blocked"
Range5	"Blocked"
Range6	"Blocked"
Range7	"Blocked"
Range8	"Blocked"

If multiple namespaces are created, then locking of all are controlled together.

Multiple Locking Ranges

Opalite	
Range	Namespace
Global	NS1
Pyrite	
Range	Namespace
Global	NS1
Opal	
Range	Namespace
Global	NS1
Range1	NS1
Range2	NS1
Range3	NS1
Range4	NS1
Range5	NS1
Range6	NS1
Range7	NS1
Range8	NS1

If multiple Locking ranges are configured, then they all are within a single namespace, and additional namespaces cannot be created.

WIP to align with NVMe to enable a strong collaboration between the organizations.

*Other names and brands may be claimed as the property of others.

Configurable Namespace Locking Feature Set

- Introduces new mechanism to assign locking range(s) to namespaces
- Allows for 1 or more locking ranges per namespace, each with individual access control and media encryption keys
- Made to work dynamically with Namespace Management use cases in mind

Range	Namespace
Global	NS1 NS3 NS7
Range1	NS2
Range2	NS4
Range3	NS4
Range4	NS5
Range5	NS6
Range6	NS6
Range7	NS8
Range8	NS9

One or more locking ranges associated with “configured” namespaces, allowing these namespaces to be unlocked separately, with differently configurable access controls.

*Other names and brands may be claimed as the property of others.

Questions?

- Thank you!