Securing Flash and Solid State Drives

Dr. Marco A.A. Sanvido
Hitachi Global Storage Technologies
(Trusted Computing Group)
Marco.sanvido@hitachigst.com

August 11th, 2009

Why Securing Flash

- Specific Requirements? Yes!!!
  - Confidentiality: an attacker can easily read data. Although wear-leveling can be considered a random permutation of the data block this is only obfuscation.
  - Integrity: an attacker can easily modify data blocks.
  - Access Control: NAND Flash does not provide any access control.

Why Security in Flash Storage?

3 Simple Reasons

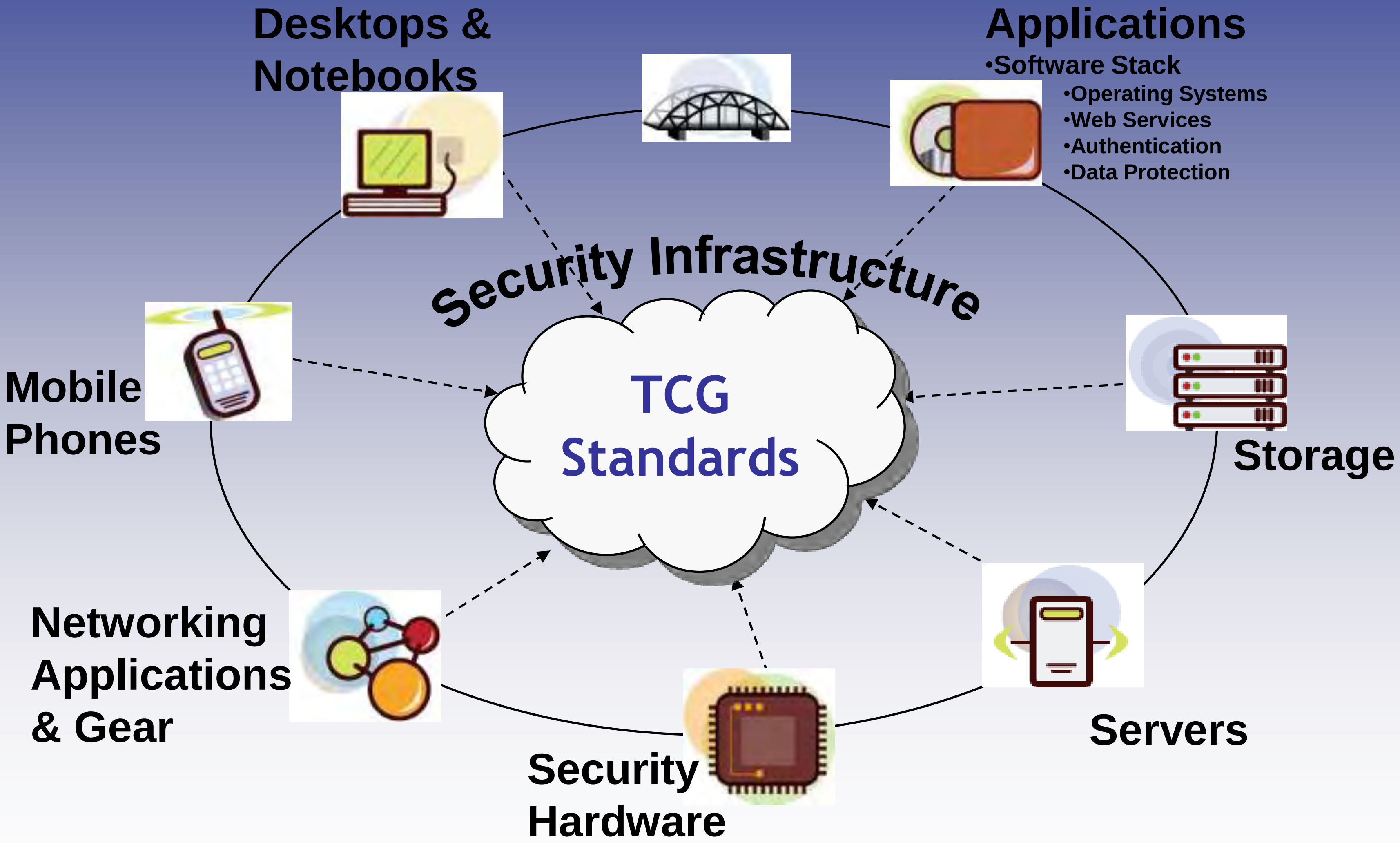
- Storage for secrets with strong access control
  - Arbitrarily large memory space
  - Gated by access control
- Unobservable cryptographic processing of secrets
  - Processing unit “welded” to storage unit
  - “Closed”, controlled environment
- Custom logic for faster, more secure operations
  - Inexpensive implementation of modern cryptographic functions
  - Complex security operations are feasible

Securing Flash Storage

- Storage Security is not only about encryption:
  - Is a about:
    - Confidentiality
    - Integrity
    - Access Control
    - Key Management
    - Online and Offline
    - …..

Requires a platform capable of accommodating
all these requirements.
Moreover in order to enable a storage security ecosystem
a standardized platform is necessary.

Trusted Computing Group



Desktops & Notebooks

Applications

- Software Stack
  - Operating Systems
  - Web Services
  - Authentication
  - Data Protection

Security Infrastructure

TCG Standards

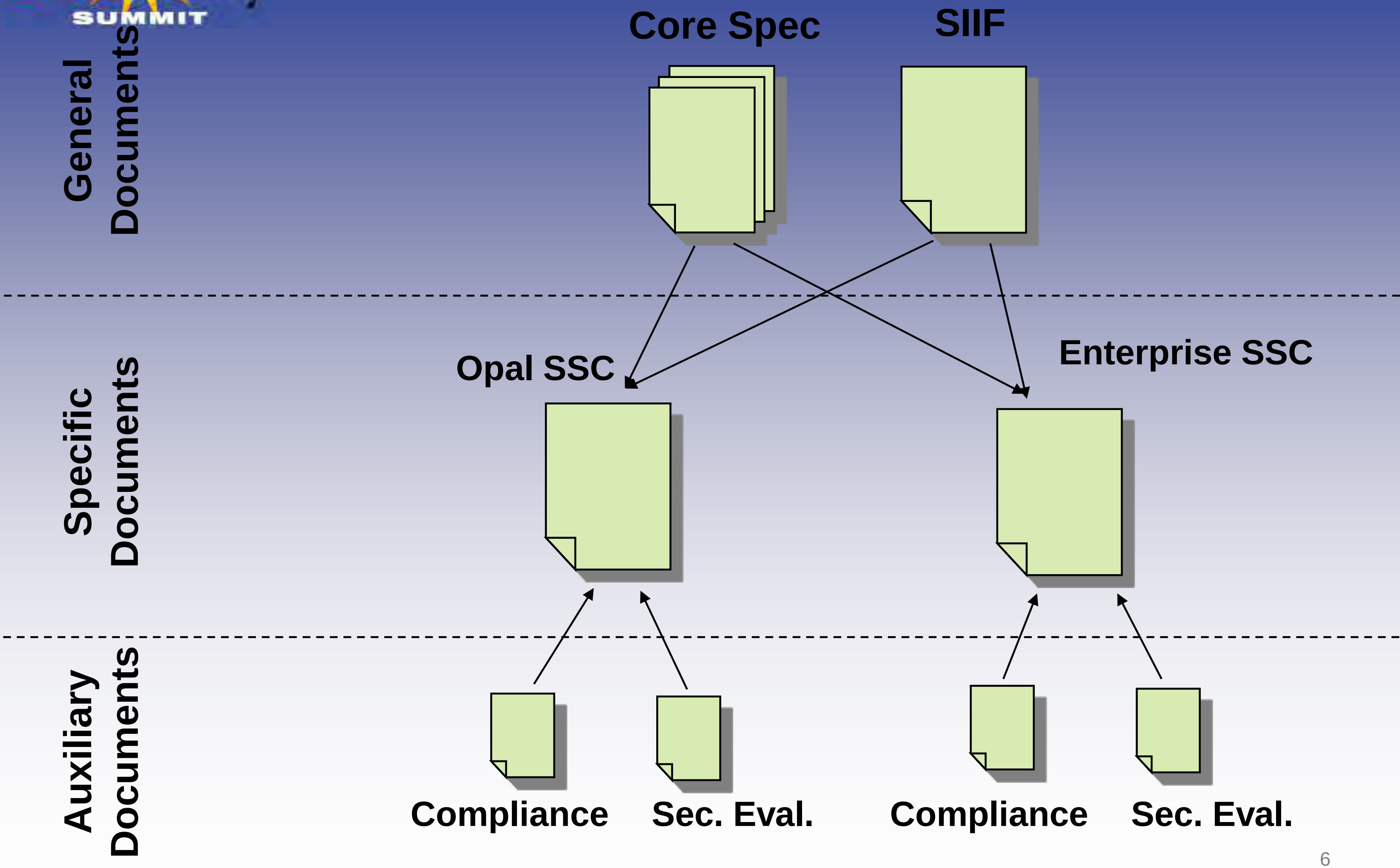
Mobile Phones

Storage

Networking Applications & Gear

Security Hardware

Servers



General Documents

Specific Documents

Auxiliary Documents

Core Spec

SIIF

Opal SSC

Enterprise SSC

Compliance

Sec. Eval.

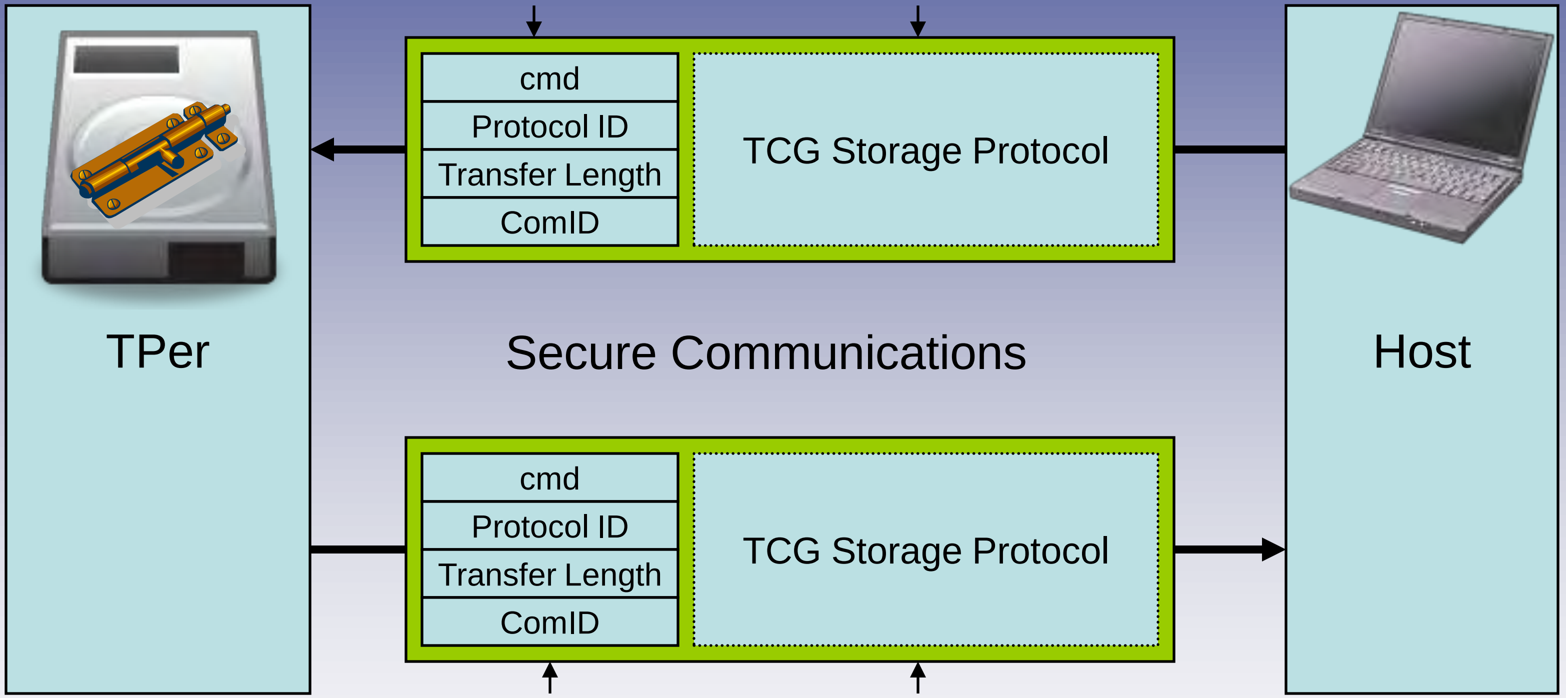
Compliance

Sec. Eval.

Storage-to-Host Communications

Trusted-Send/Secure Out command block

Trusted Send/Secure Out data block



cmd

Protocol ID

Transfer Length

ComID

TCG Storage Protocol

TPer

Secure Communications

Host

cmd

Protocol ID

Transfer Length

ComID

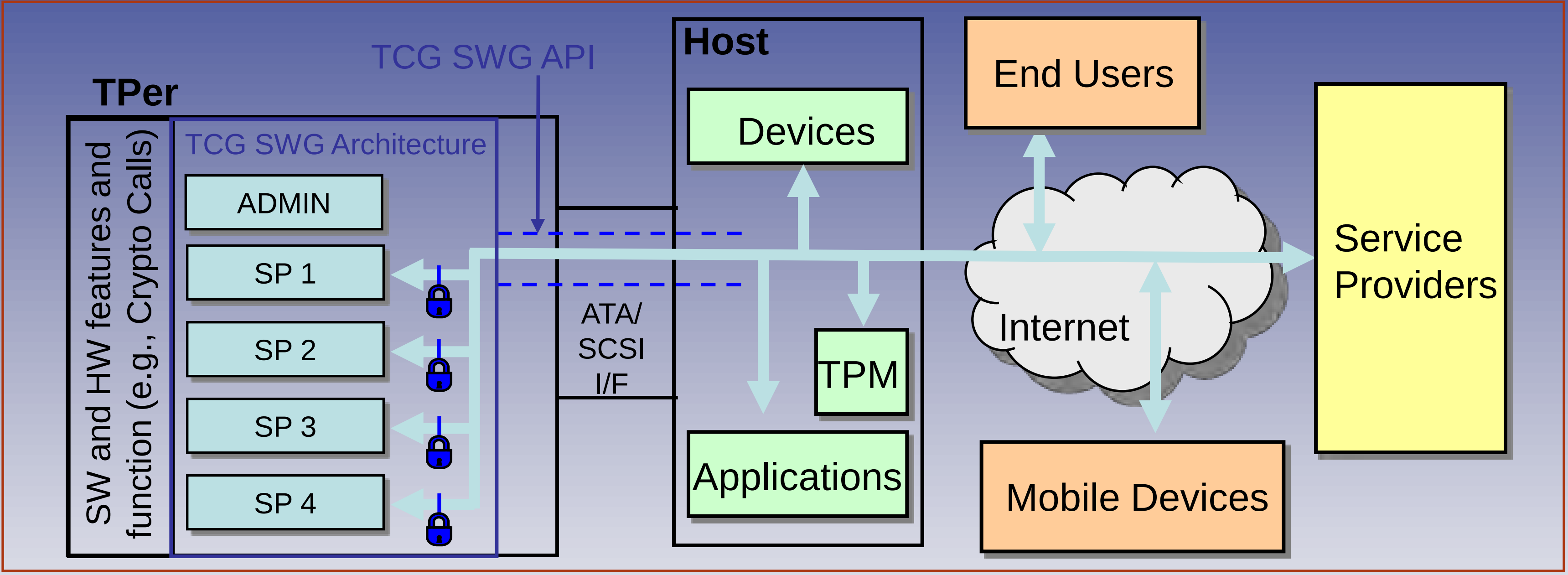
TCG Storage Protocol

Trusted Receive/Secure In command block

Trusted Receive/Secure In data block

ComID: allows TPer to identify caller of Trusted Receive/Secure In command

TCG Storage Work Group: Overview

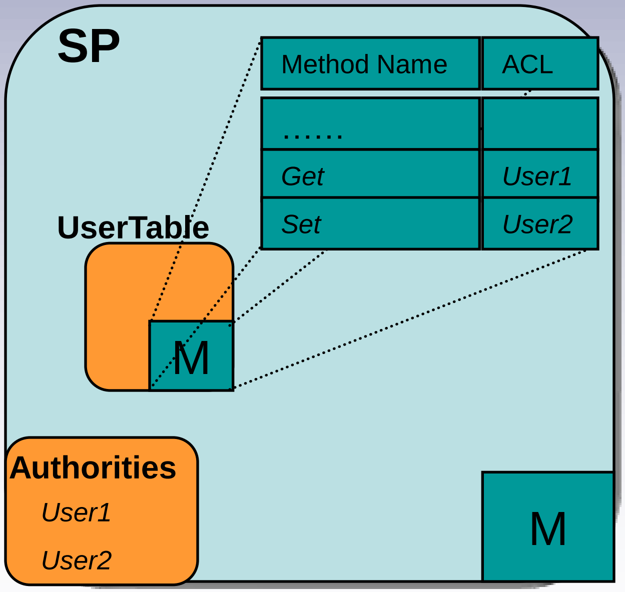


The host platform, applications, devices, local end users, and remote users/service providers can gain exclusive control of selected features of the storage device. This allows them to simultaneously and independently extend their trust boundary into the storage device or trusted peripheral (TPer)

TCG Storage Work Group: Architecture

Storage Work Group specifications are intended to provide a comprehensive command architecture for putting selected features of storage devices under policy-driven access control.

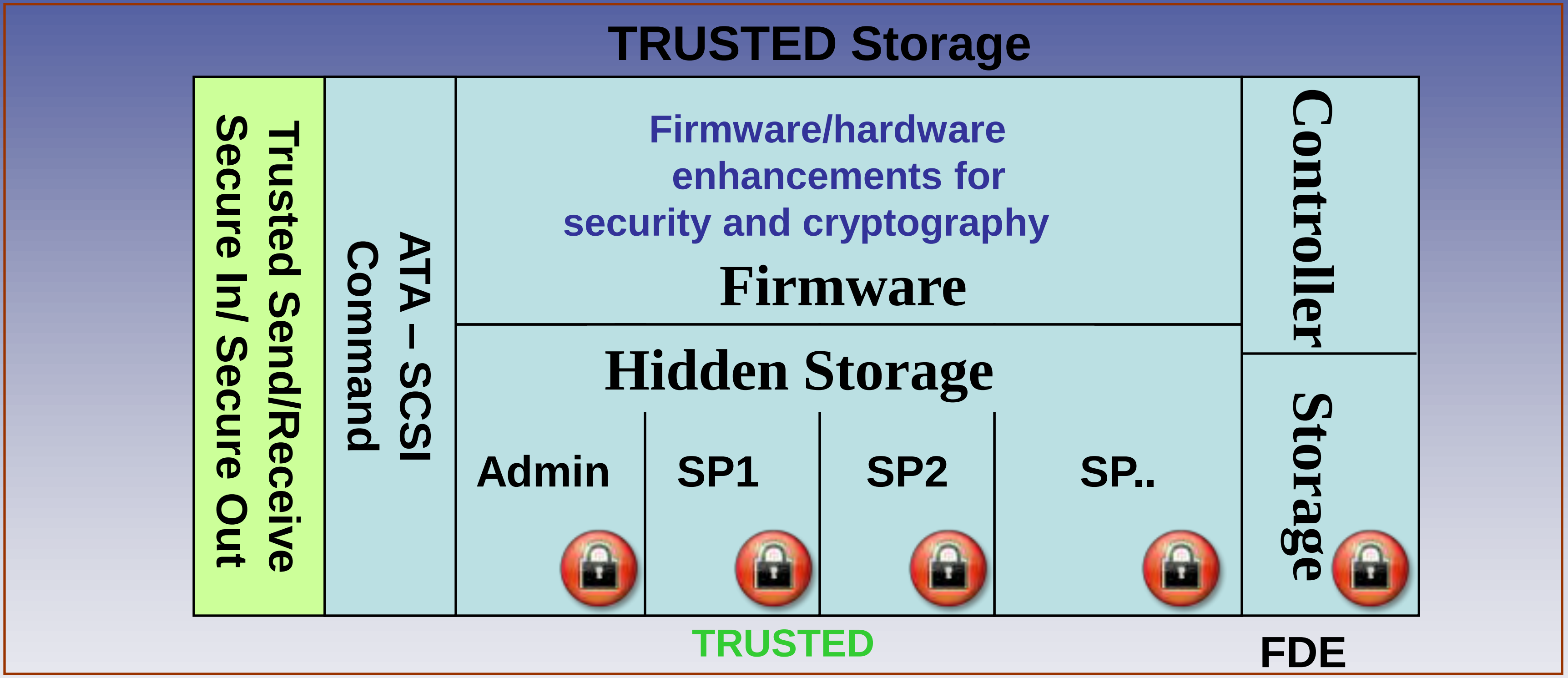
- Features will be packaged into individual functionality containers called: “Security Providers” or SPs.



Method Name	ACL
……	
Get	*User1*
Set	*User2*

- Each SP is a “sand box” exclusively controlled by its owner. SP functionality is a combination of pre-defined functionality sets called SP Templates:
  - Base
  - Admin
  - Crypto
  - Log
  - Clock
  - Locking
- SPs are a collection of tables and methods that control the persistent trust state of the TPer.
  - Method invocation occurs under access control.
  - The SP has a list of authorities and their respective credentials for access control.

TCG Storage Work Group: Implementation Overview



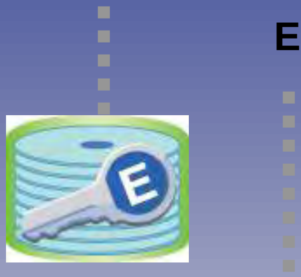
- (Partitioned) Hidden Storage
- Security firmware/hardware
- Trusted Container Commands

Core Architecture Incarnations: Security Subsystem Classes

- The Core Specification defines a comprehensive set of security features, but not all are necessary to implement a security solution.
- An SSC defines such a subset addressed to a particular set of requirements/market.
- Currently under development:
  - NB Market / HDD Loss & Theft (Opal SSC)
  - Enterprise: Band Encryption and re-purposing (Enterprise SSC)

Enterprise SSC Overview

- Threat Model
  - Lost / Stolen Drives
- Features
  - Encryption
  - Drive Locking with PW access control
  - Encryption Ranges
  - (Fast Secure Erase)

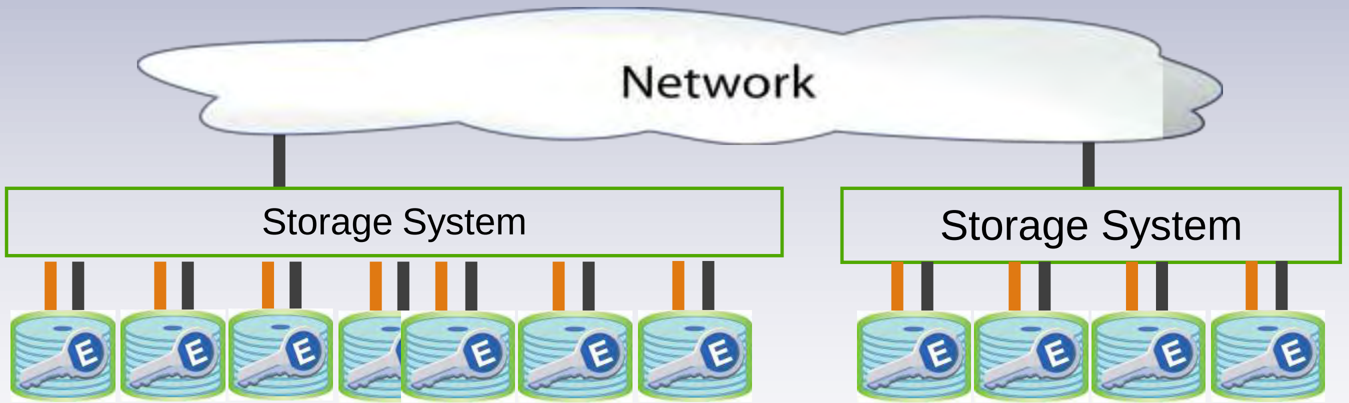


Encryption engine speed

Matches

Port's max speed

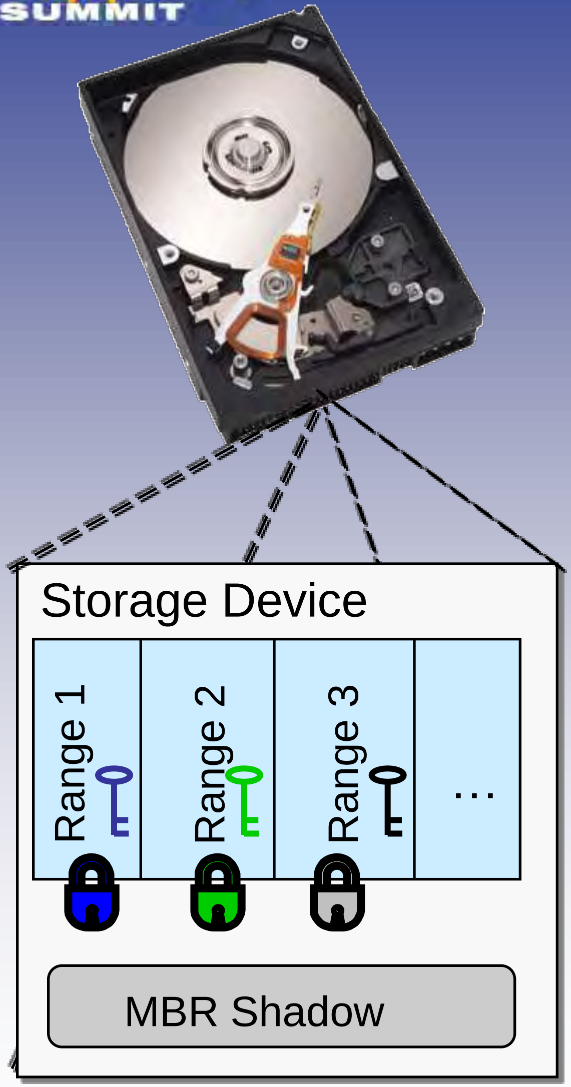
Scales Linearly, Automatically



All data can be encrypted, with no performance degradation

Less need for data classification

Opal SSC Overview



Storage Device

Range 1

Range 2

Range 3

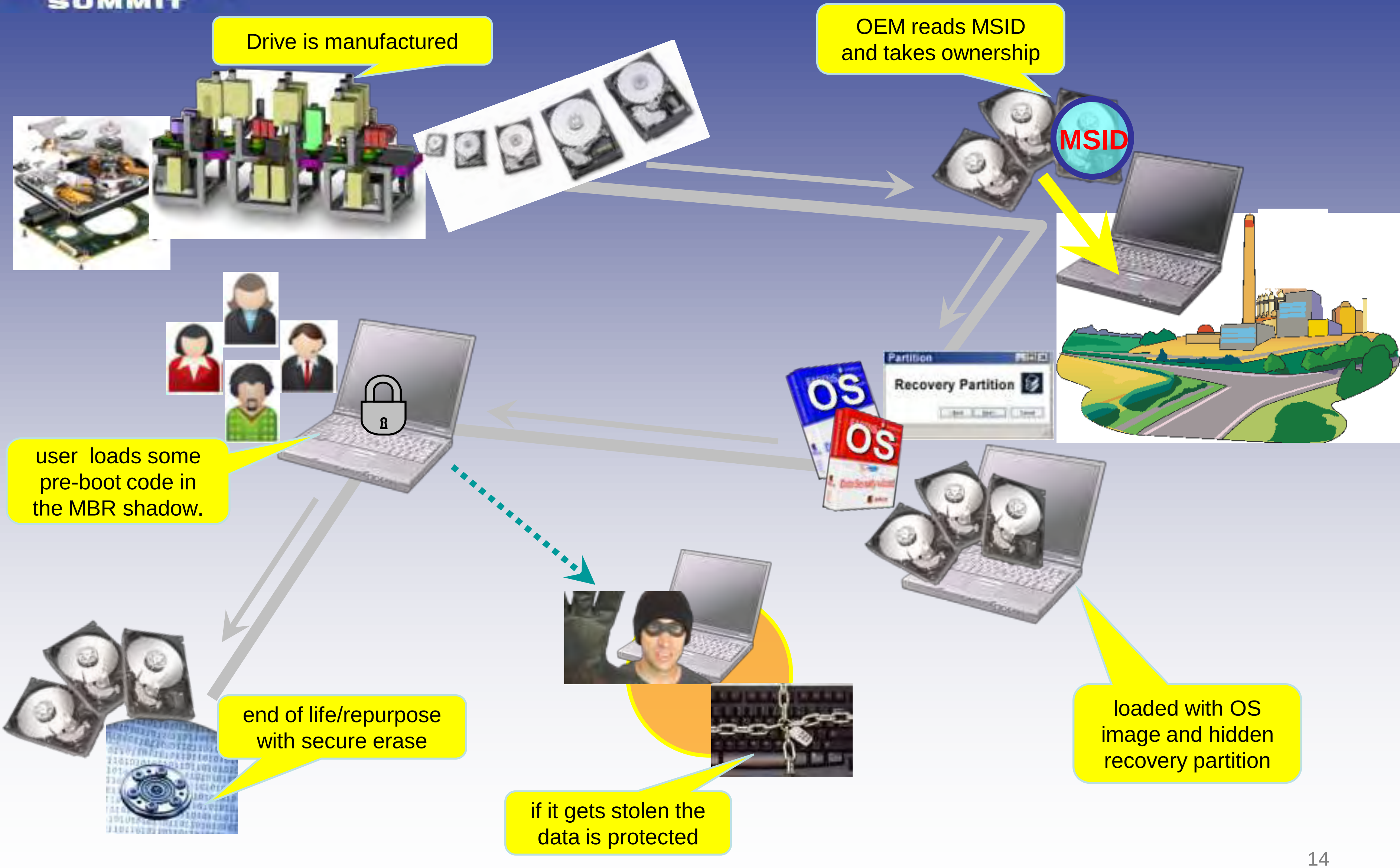
…

MBR Shadow

- Threat Model
  - Lost / Stolen Laptops
  - (Offline leakage of data)
- Features
  - Encryption
  - Drive Locking with PW access control
  - Encryption Ranges
  - MBR Shadowing (Pre-Boot)
  - (Fast Secure Erase)

- Very simple to use SSC addressing PC Client system needs.

Example Life of an Opal HDD



Drive is manufactured

OEM reads MSID and takes ownership

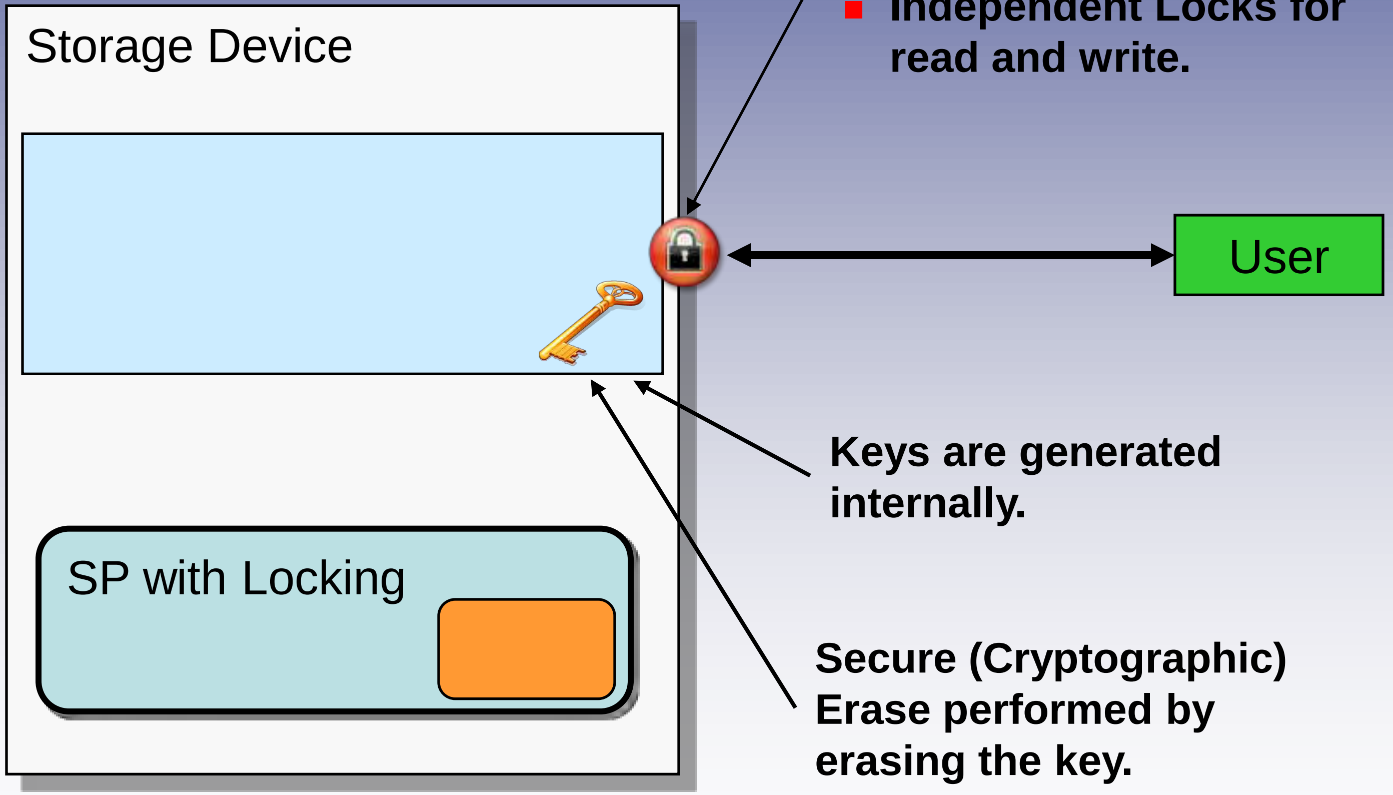
loaded with OS image and hidden recovery partition

user loads some pre-boot code in the MBR shadow.

if it gets stolen the data is protected

end of life/repurpose with secure erase

Encryption/Locking



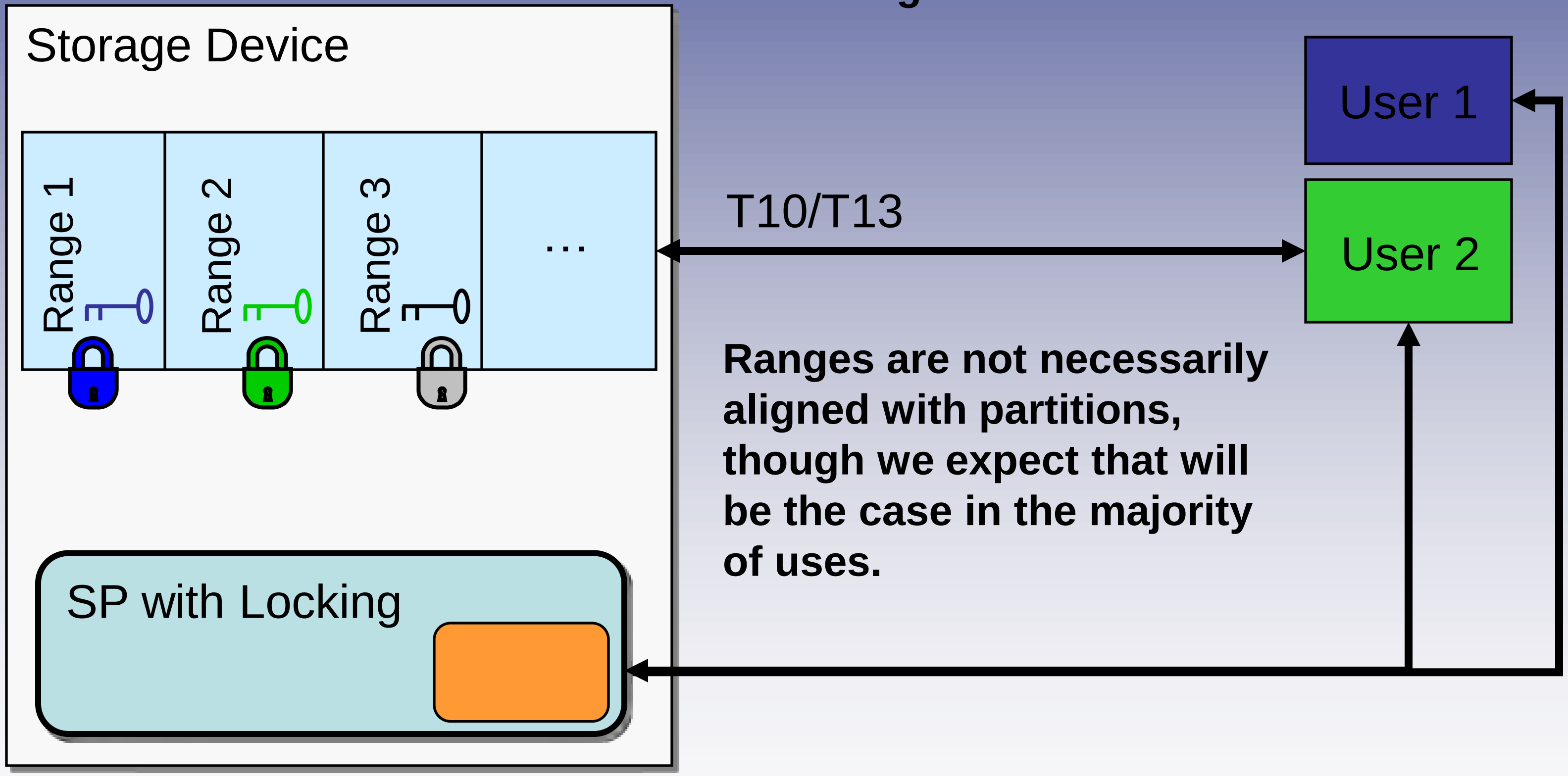
- Access control for locking and unlocking
- Independent Locks for read and write.

Keys are generated internally.

Secure (Cryptographic) Erase performed by erasing the key.

Ranges

Independent encryption and access control for each range.

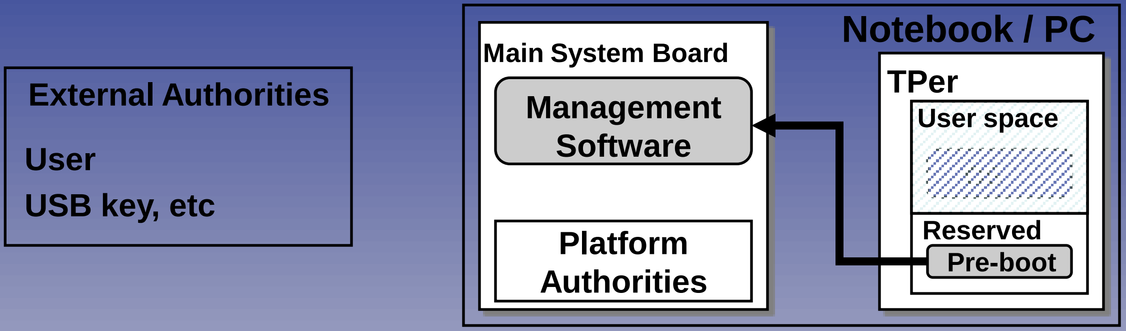


Ranges are not necessarily aligned with partitions, though we expect that will be the case in the majority of uses.

MBR Shadowing

Initial Power-up

- When the system first requests the MBR, the HDD returns the pre-boot code (the MBR shadow).



External Authorities

User

USB key, etc

Notebook / PC

Main System Board

Management Software

Platform Authorities

TPer

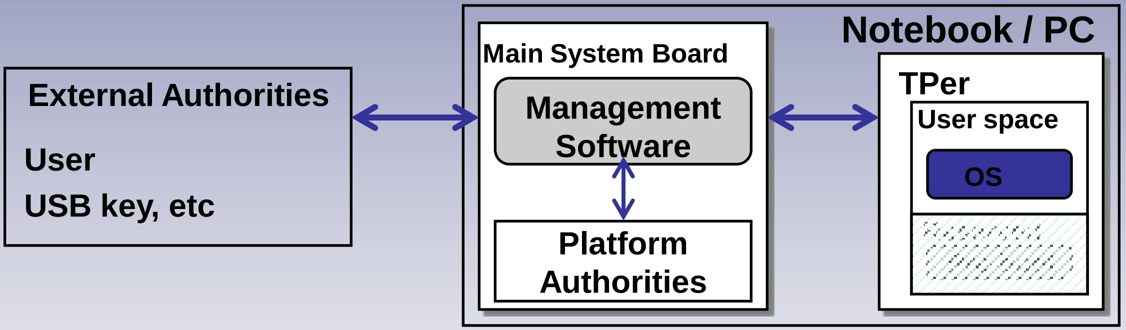
User space

Reserved

Pre-boot

Authentication and Unlock

- The pre-boot code manages the authentication process with both internal and external authorities.
- After the appropriate authentications, the management software unlocks the regular user space.



External Authorities

User

USB key, etc

Notebook / PC

Main System Board

Management Software

Platform Authorities

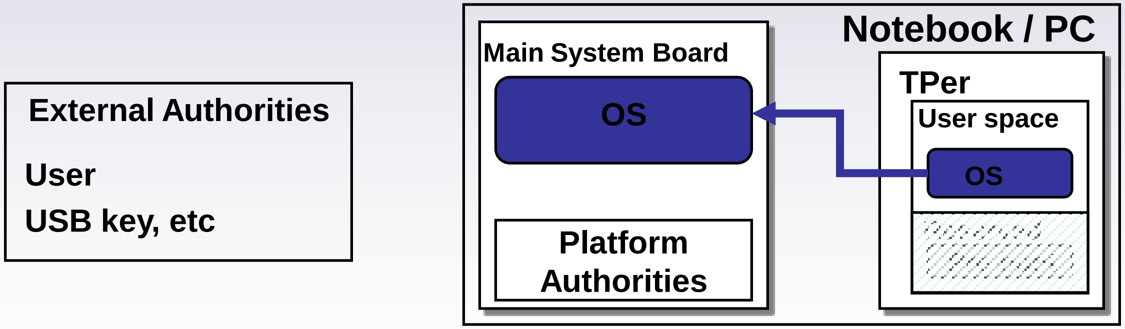
TPer

User space

OS

Resume Normal Boot

- After the HDD is unlocked, the management software sends the system back to the boot process.
- The system’s request for the MBR now returns the true MBR and the OS is loaded completing the boot process.



External Authorities

User

USB key, etc

Notebook / PC

Main System Board

OS

Platform Authorities

TPer

User space

OS

THANK YOU!

www.trustedcomputinggroup.org

Core Specification v2.0:

http://www.trustedcomputinggroup.org/resources/tcg_storage_architecture_core_specification_version_200_revision_100

Opal Specification v1.0:

http://www.trustedcomputinggroup.org/resources/tcg_storage_security_subsystem_class_opal_version_100_revision_200

Enterprise Specification v1.0:

http://www.trustedcomputinggroup.org/resources/storage_work_group_storage_security_subsystem-
_class_enterpriseversion_10_revision_10