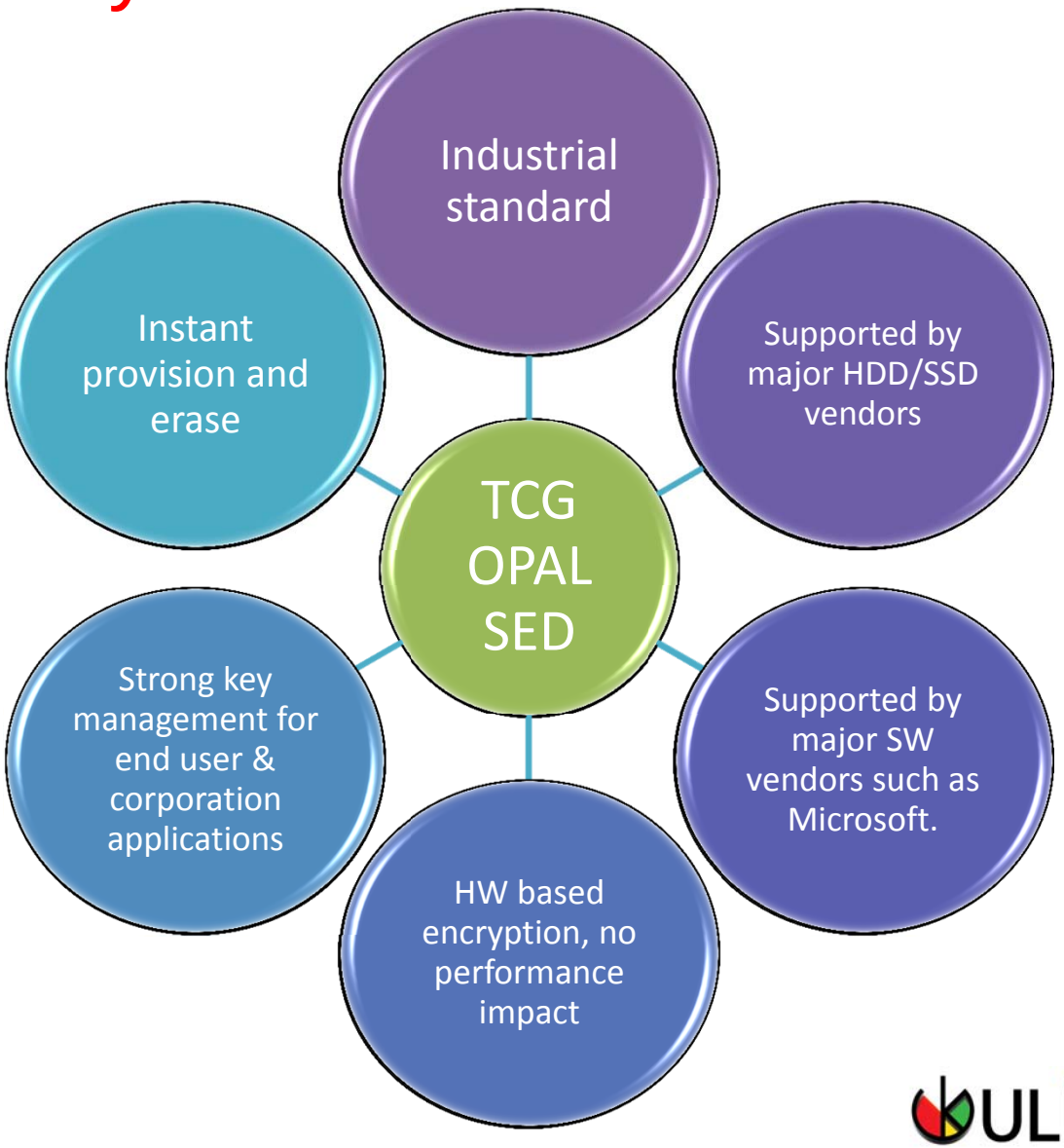
# TCG OPAL Design and Testing

FMS Session 103-A, Security

by

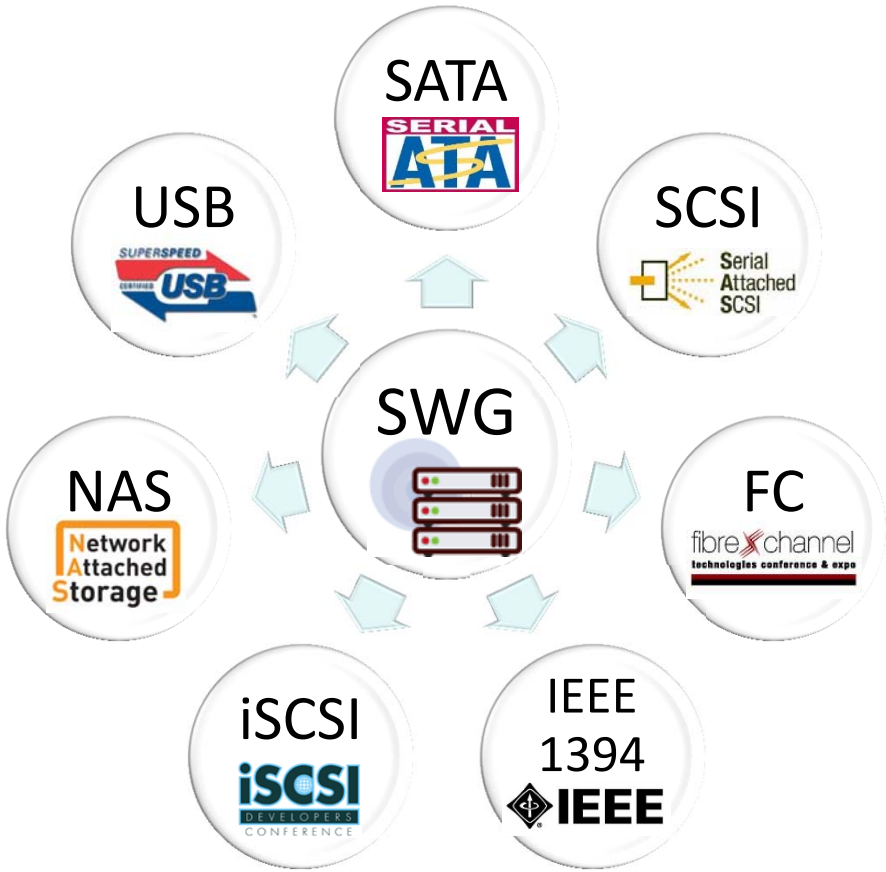
Joseph Chen, ULINK Technology

# Why TCG OPAL SED



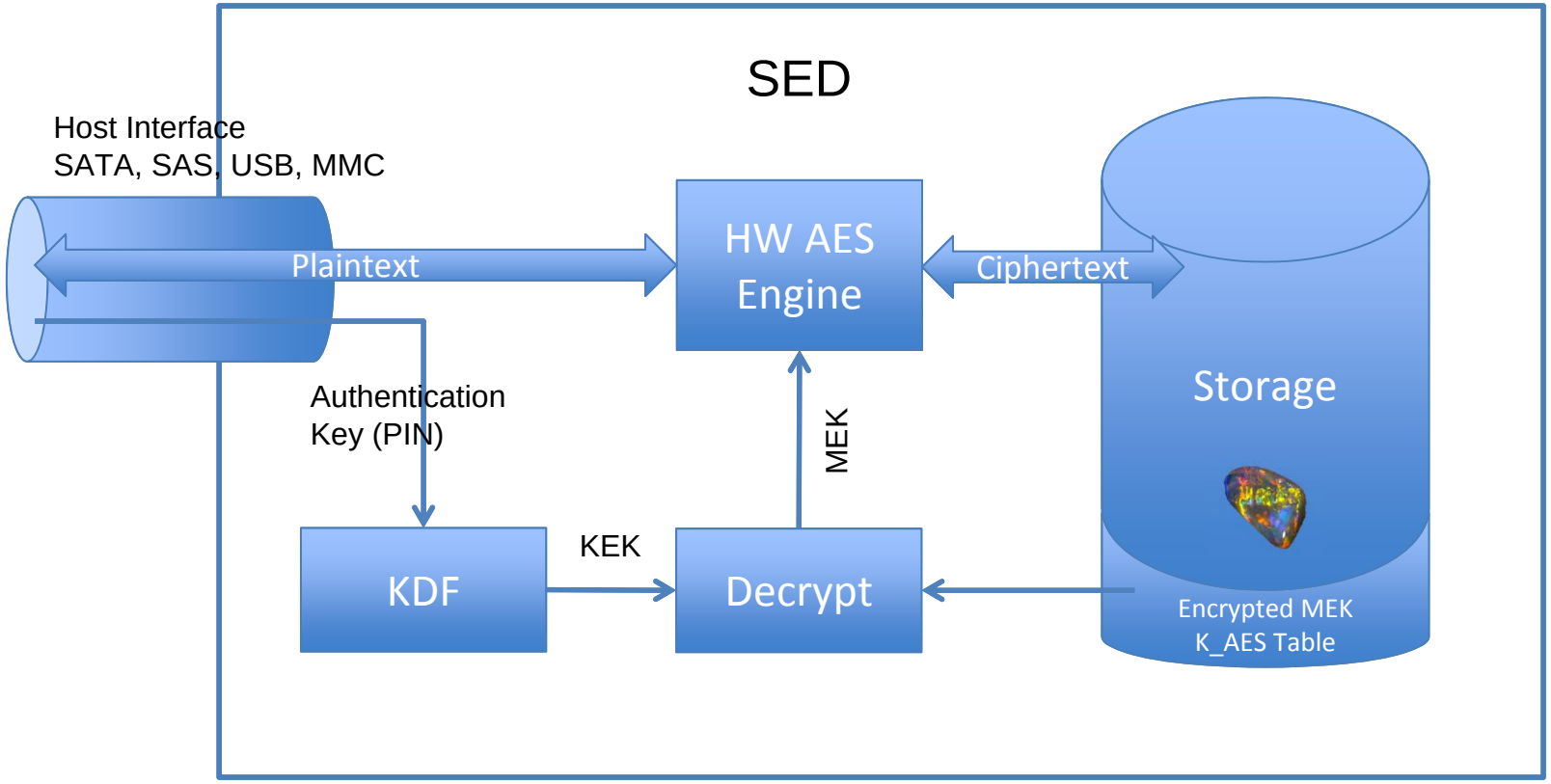
# Introduction of the TCG SWG (Storage Work Group)

- SWG builds upon existing TCG technologies and philosophy
- SWG focuses on standards for security services on dedicated storage systems.
- SWG defines a common security services for SATA, SCSI, SAS, FibreChannel, USB, IEEE 1394, NAS and iSCSI.
- Storage includes HDD, SSD, Removable Drive, Storage Server.

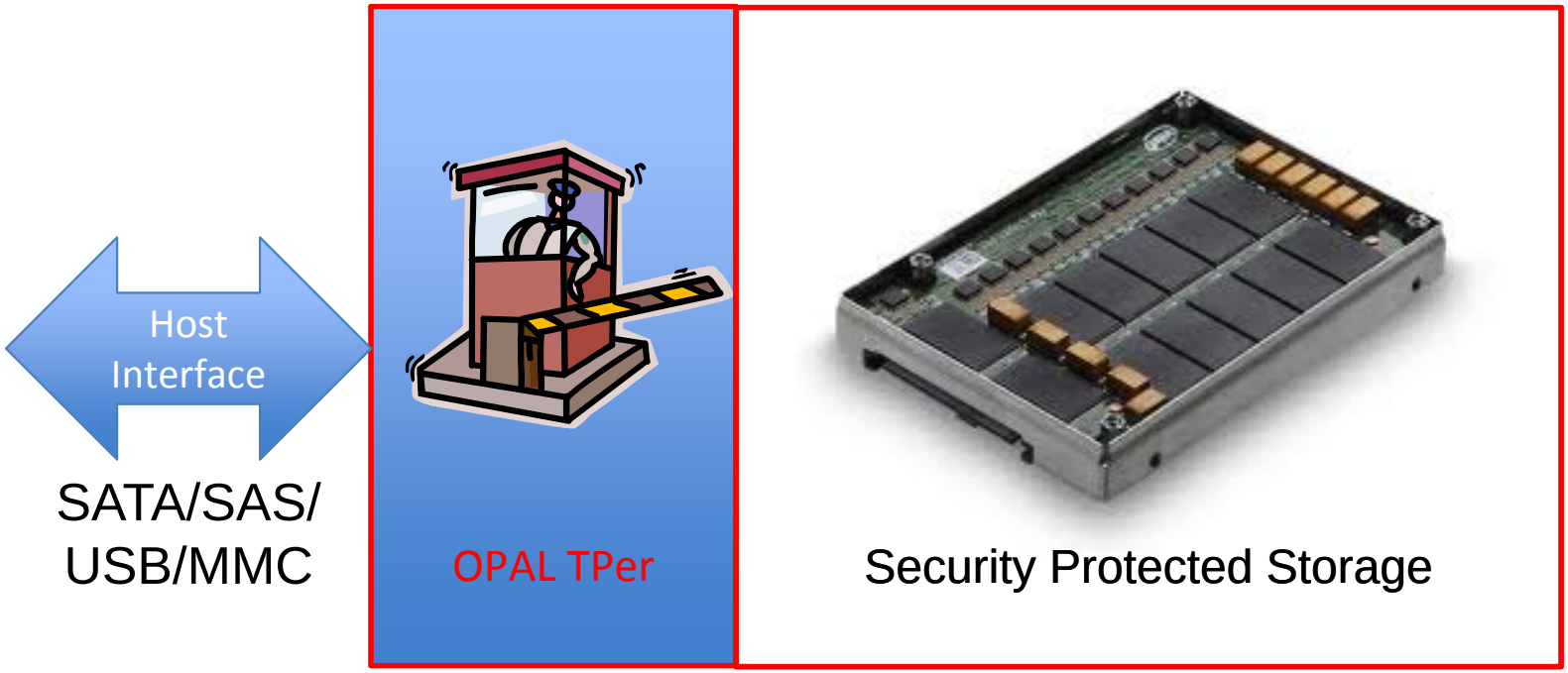



Source: TrustedComputingGroup

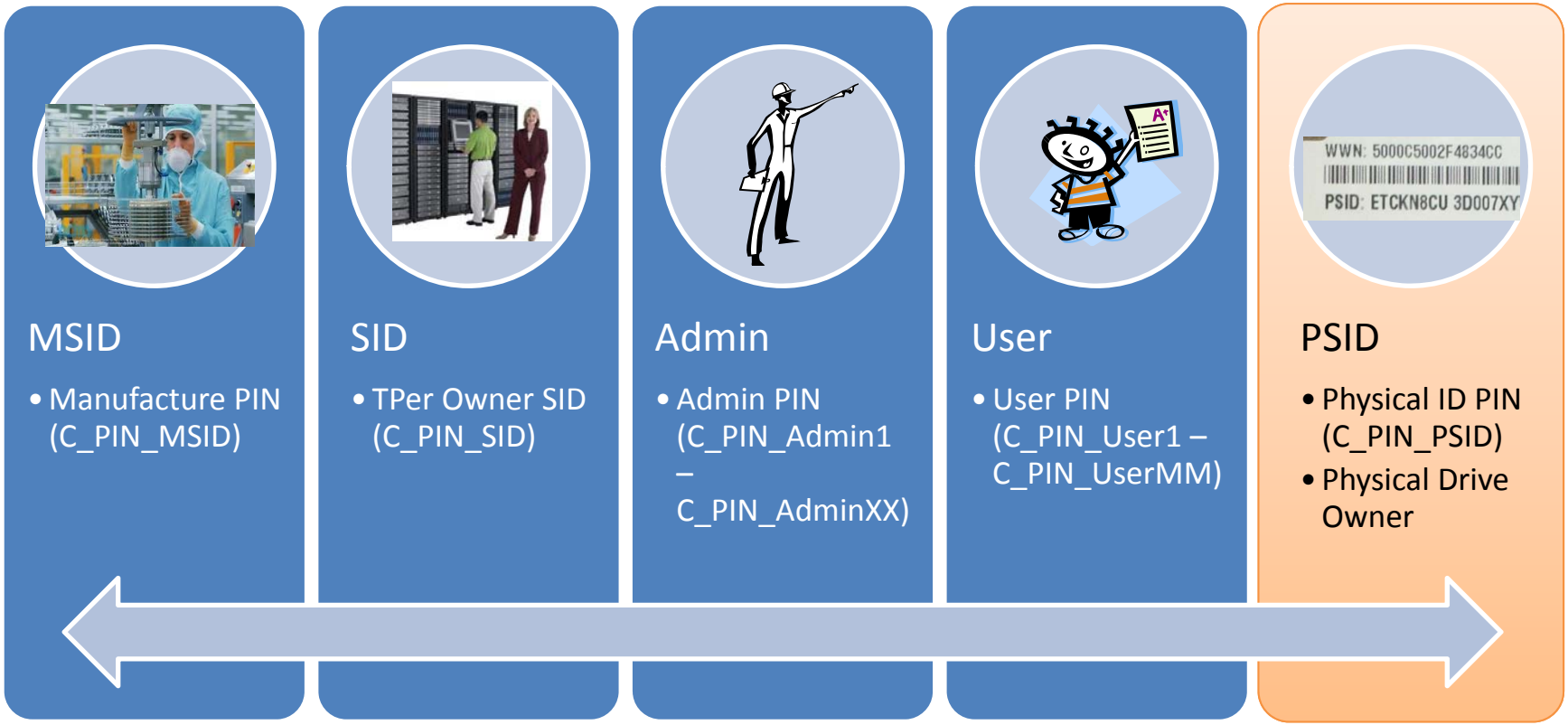
# OPAL AES Encryption Diagram



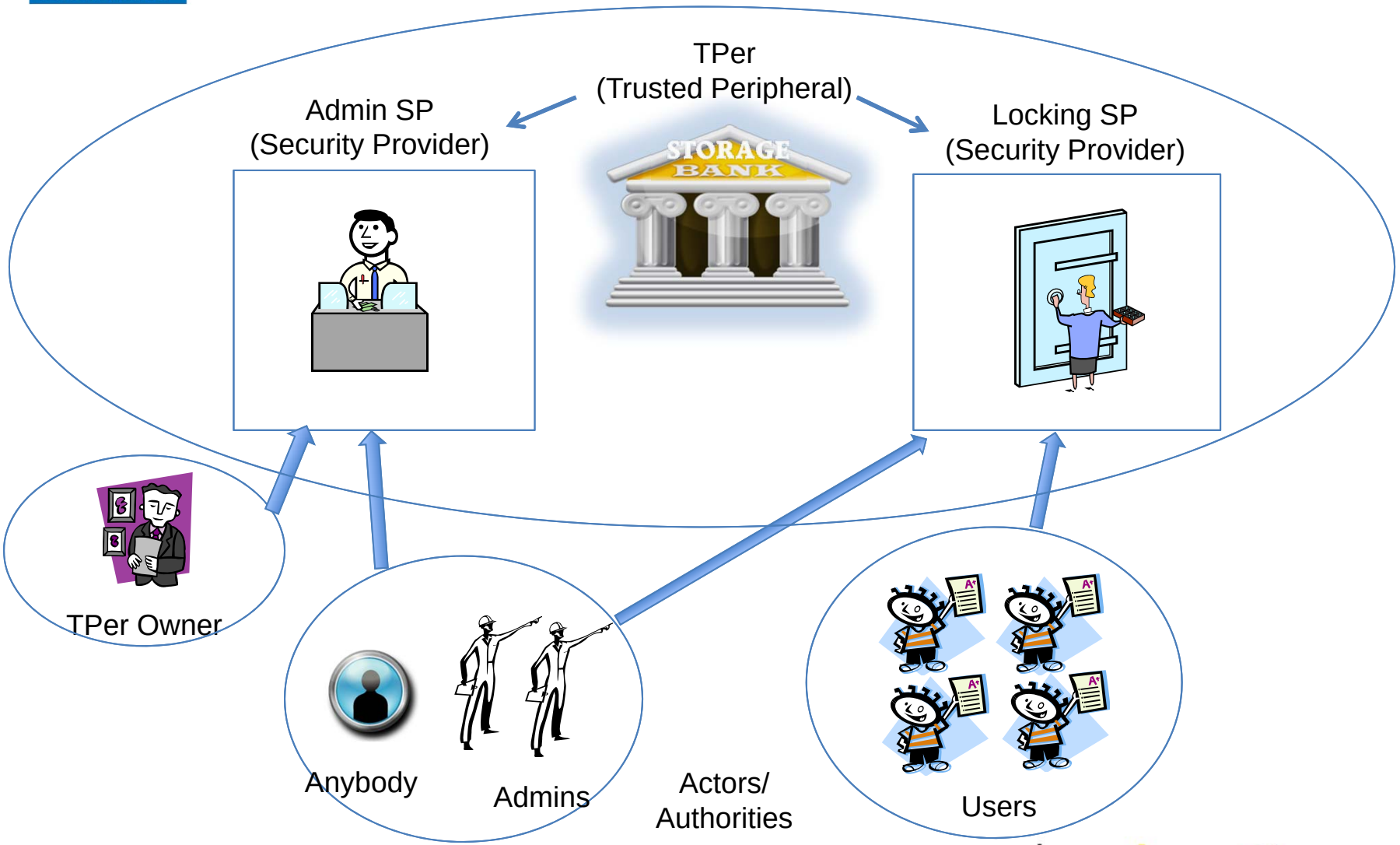
# OPAL TPer and Storage Device



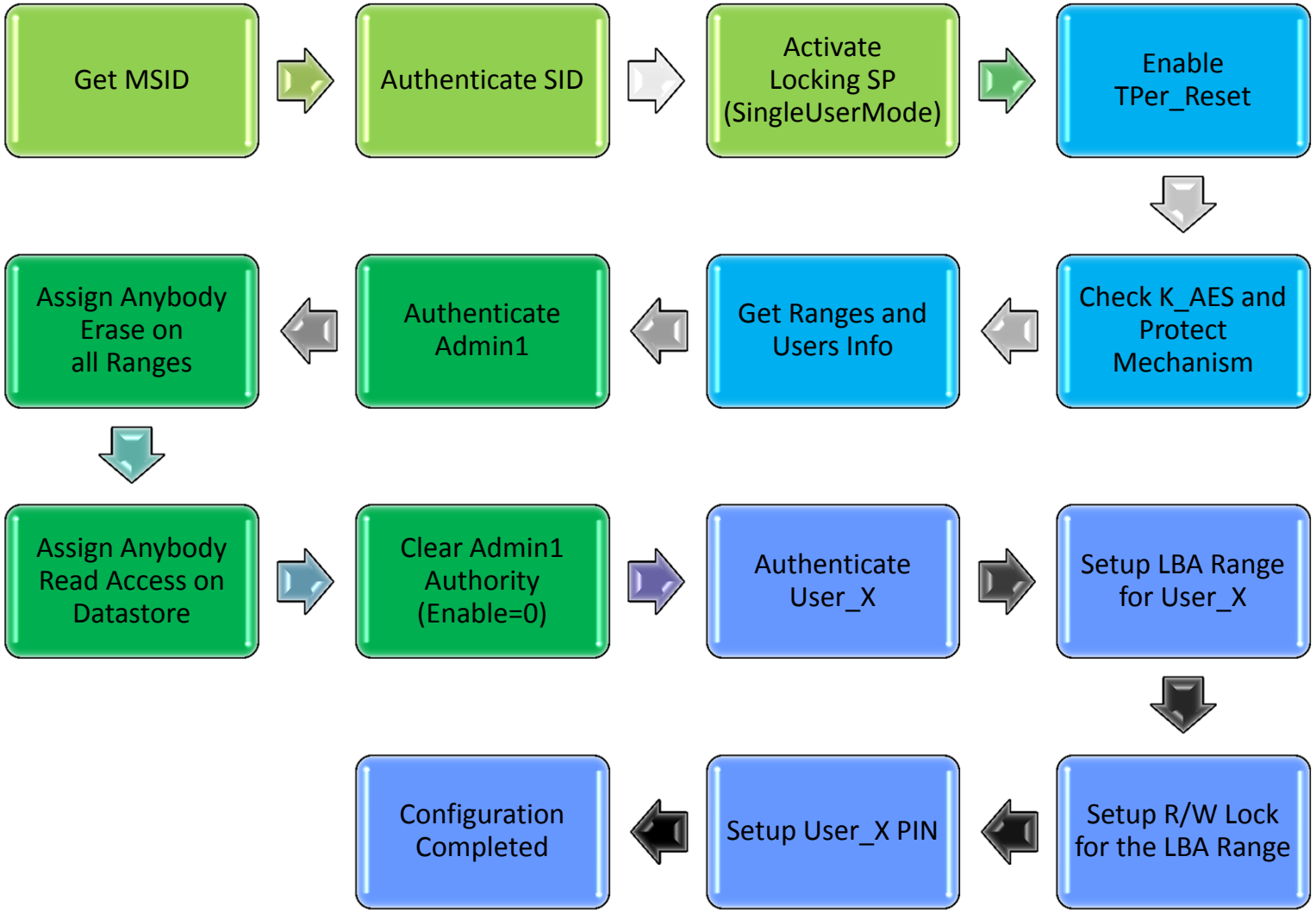
# OPAL Credentials/Authorities



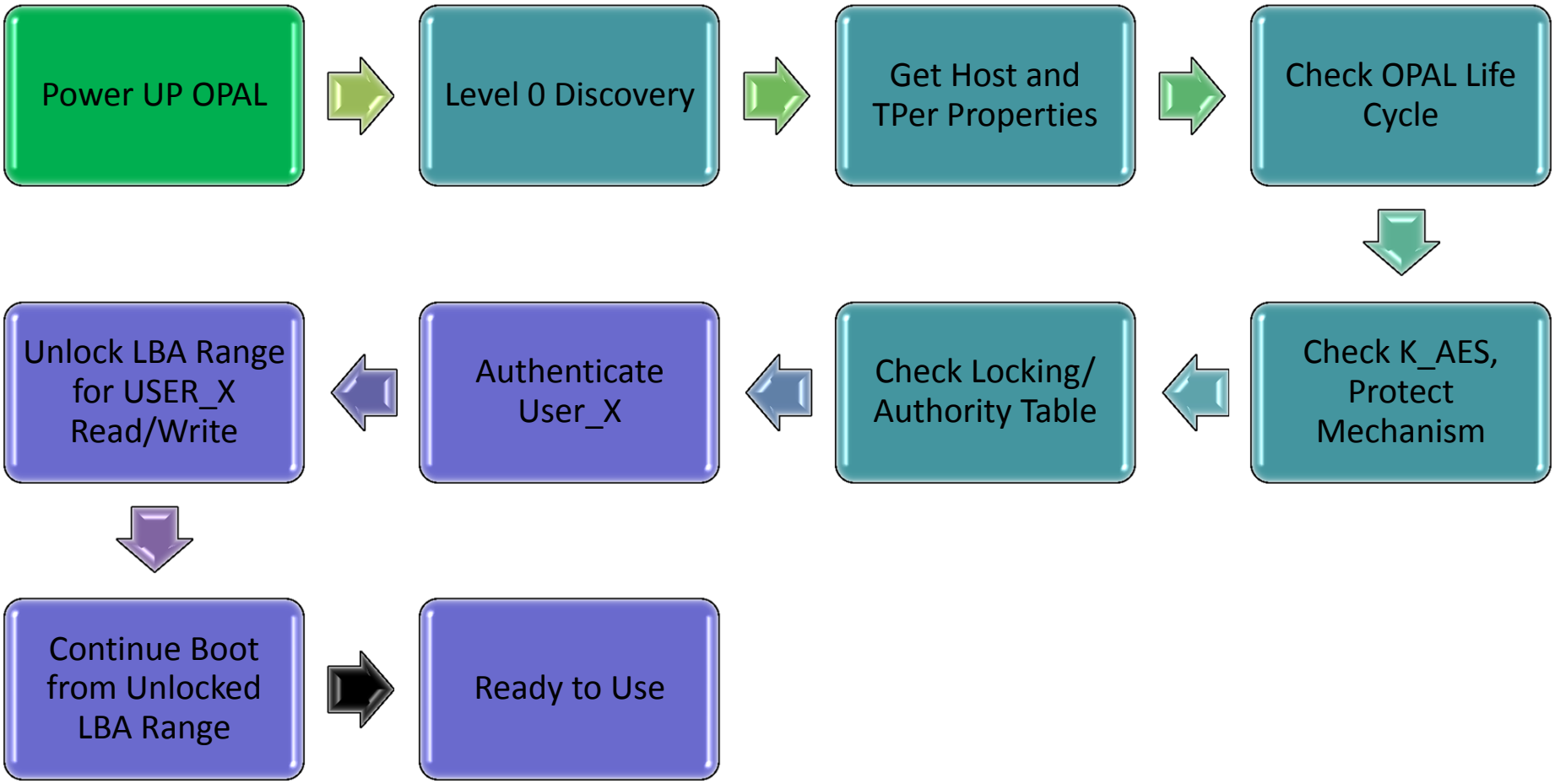
# OPAL TPer, SP and Authority



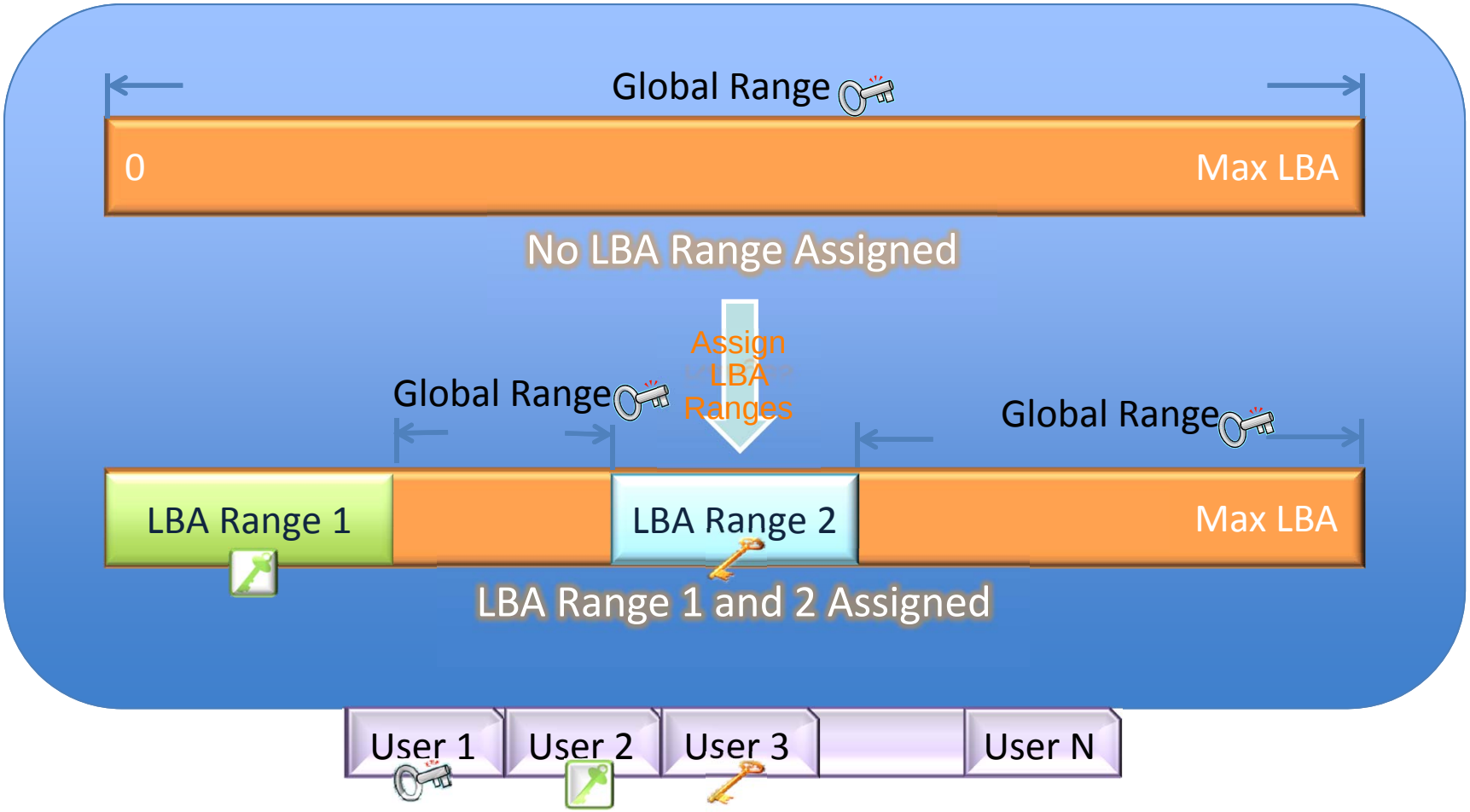
# OPAL Configuration Example



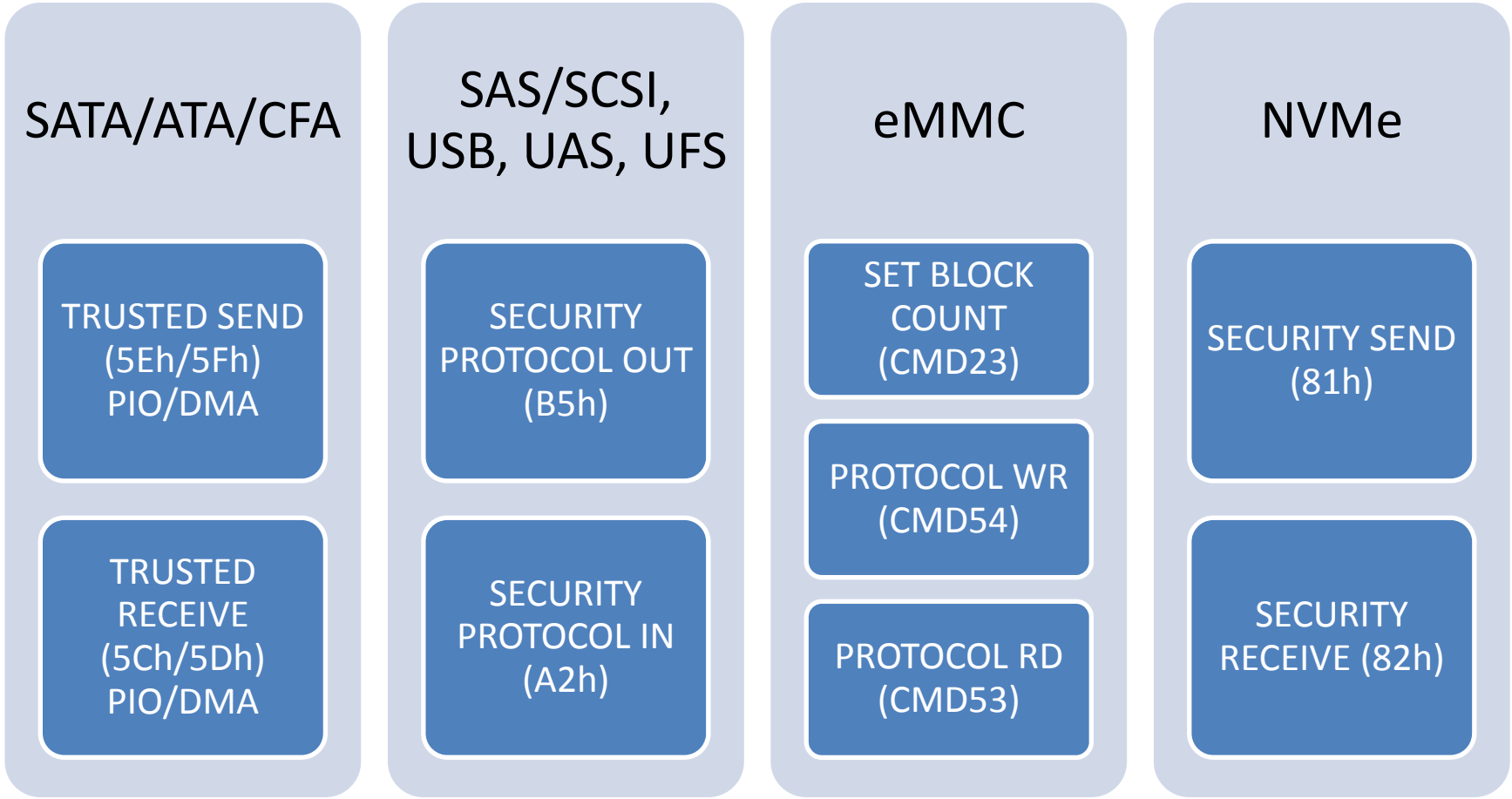
# OPAL Unlocking Example



# LBA Range Assignments Example



# OPAL Commands for SATA/SAS/USB/eMMC/NVMe



# Microsoft eDrive Requirements

## What is an eDrive?

- A regular storage subsystem (Embedded MultiMediaCard, solid-state drive, hard disk drive, usb) that comes with hardware offload to accelerate crypto processing

## How is it different from SEDs?

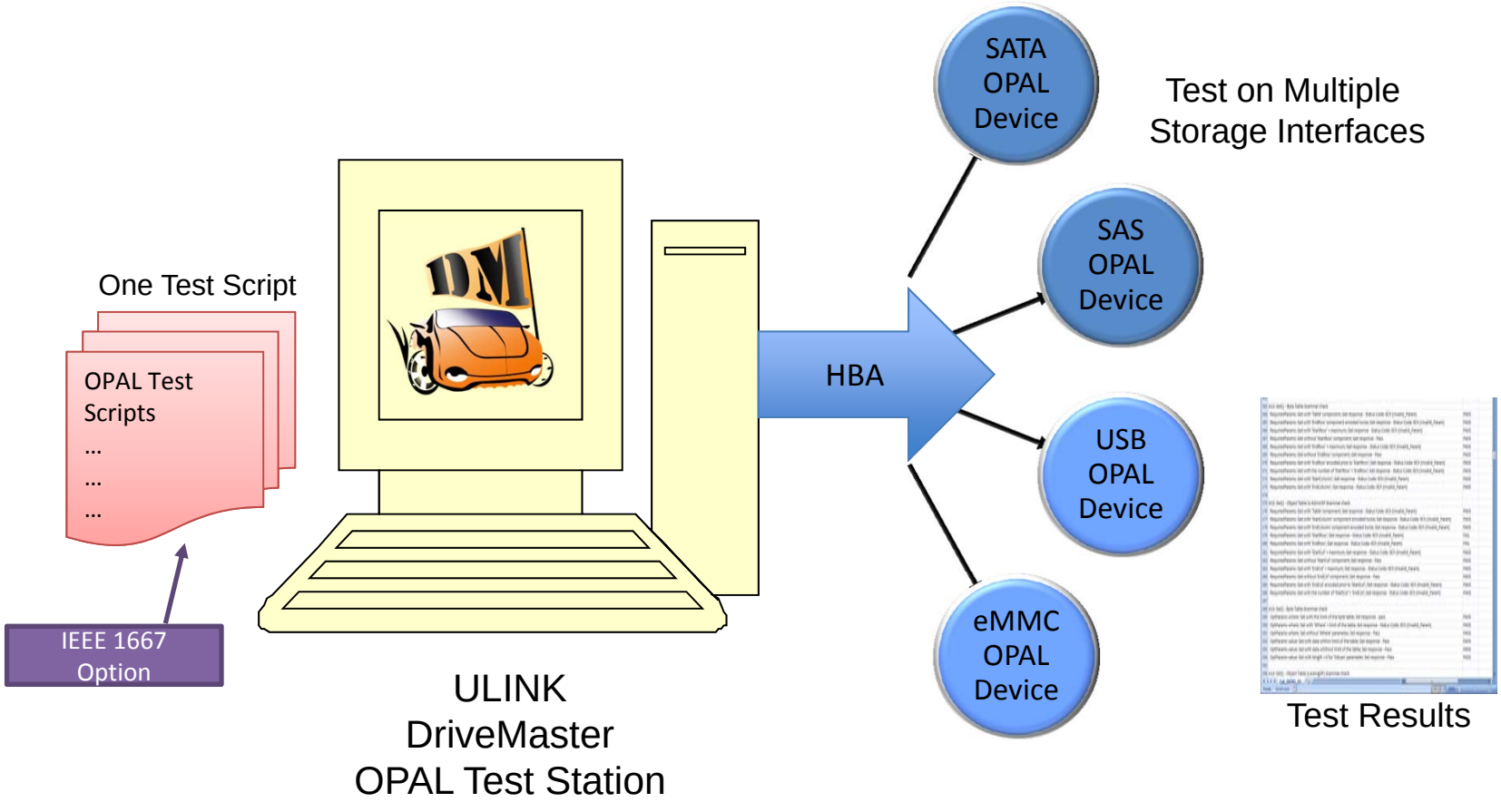
- Self-encrypting drive: Trusted Computing Group (TCG) standards
- Encrypted drive: TCG standards (OPAL v2.0) + IEEE 1667

## Why should the ecosystem care?

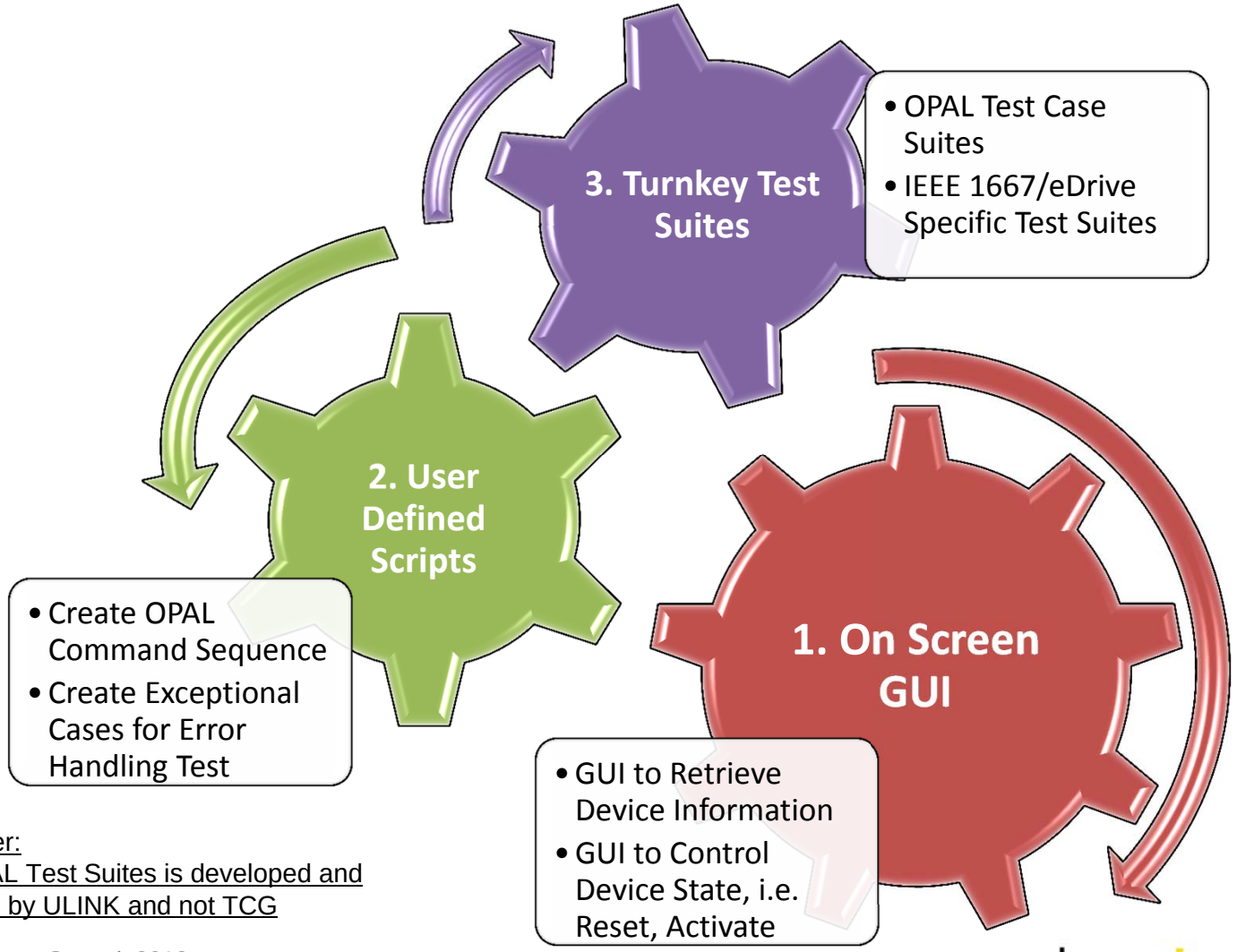
- Initial-time hardware-based encryption is negligible
- Faster than software-based encryption during standard operation
- Removes initial and on-going performance hit
- Standardized in-box support can enable broad adoption

Source from Microsoft

# DriveMaster
# OPAL Test for Multiple Interfaces



# DriveMaster Testing Applications




Disclaimer:
This OPAL Test Suites is developed and managed by ULINK and not TCG

# ULINK OPAL Workshop

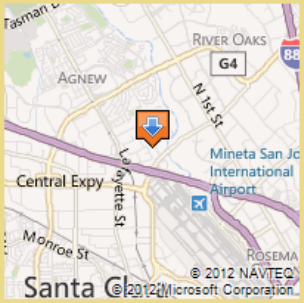
ULINK

*Contact*

Yudy Syukur
ULINK Technology, Inc.
yudy.syukur@ulinktech.com
408-446-8455 Ext 116

*Where*

APICS - The Association for Operations Management
3150 De La Cruz Blvd Ste 200
Santa Clara, CA 95054




Driving Directions

## ULINK Technology OPAL Testing Tutorial Workshop - September 11 & 12, 2012

This workshop consists of 2 sessions conducted on 2 **separate** days. Each session include a 2 hour **lecture** and a 1 hour **practice**. The tutorial topics are:

- Explanation of OPAL technology
- Explanation of Trusted Storage Architecture, the roles of Trusted Peripheral and Security Provider
- Testing / Validation methodology for OPAL devices
- Practice OPAL commands using DriveMaster tool

**When:** Tuesday Sept 11 from 1pm to 4pm (PST) **AND** Wednesday Sept 12 from 1pm to 4pm (PST)

**Fee:** $899 per person (**Register by August 14** to be eligible for a **$100 discount**)

***Each registrant will receive a **FREE Testing Service** in confidence of TCG Storage OPAL test cases v1.0 for one device. ***(This Testing Service is regularly priced at $2,000)***

Seating is limited. So please register early. *(We reserve the right to cancel the class if the number of registrants does not meet our target )*

Click in this block to add your text and images to promote your event. You can add more blocks to this Event Homepage by selecting Add Blocks above.

*Register Now!*

# Q&A

- Question?


For more information please contact

Joseph.chen@ulinktech.com

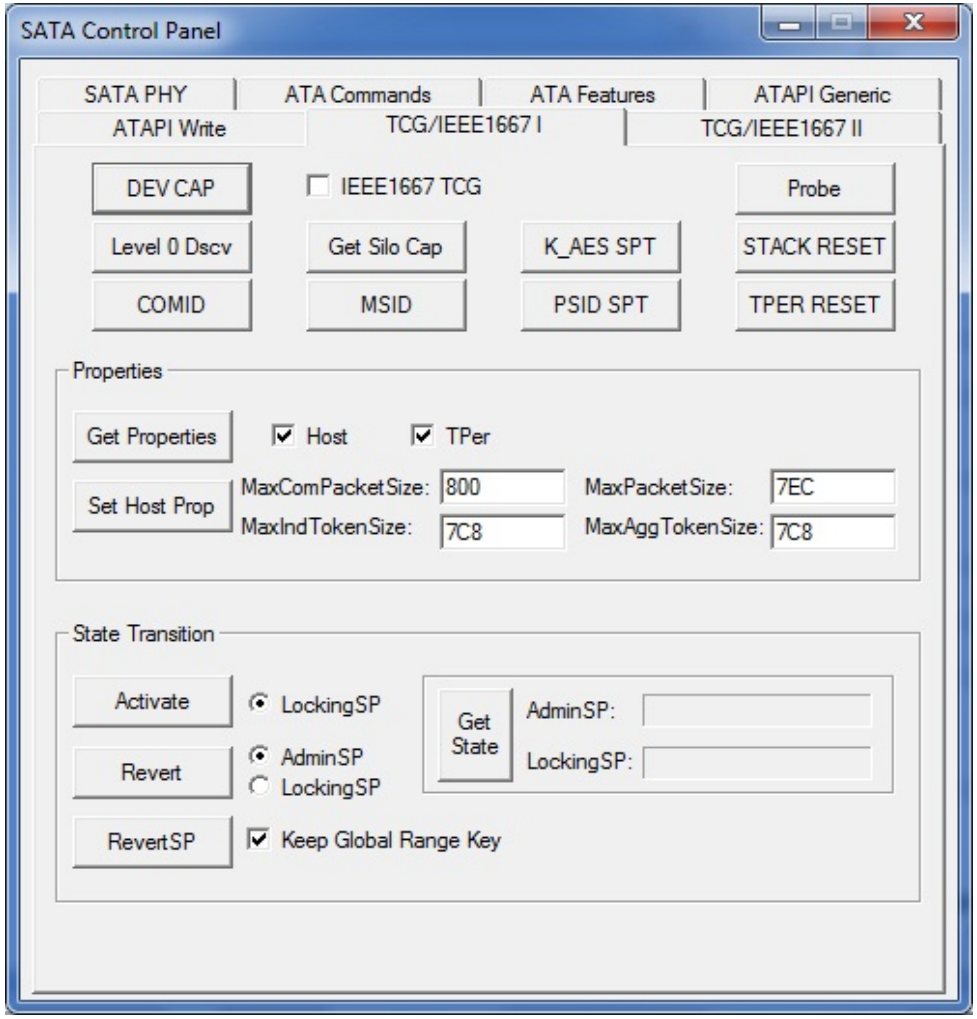
Edwin.kuo@ulinktech.com

Visit our Booth #701
In the Exhibition Hall

# ULINK – Professional Mass Storage Test Tools

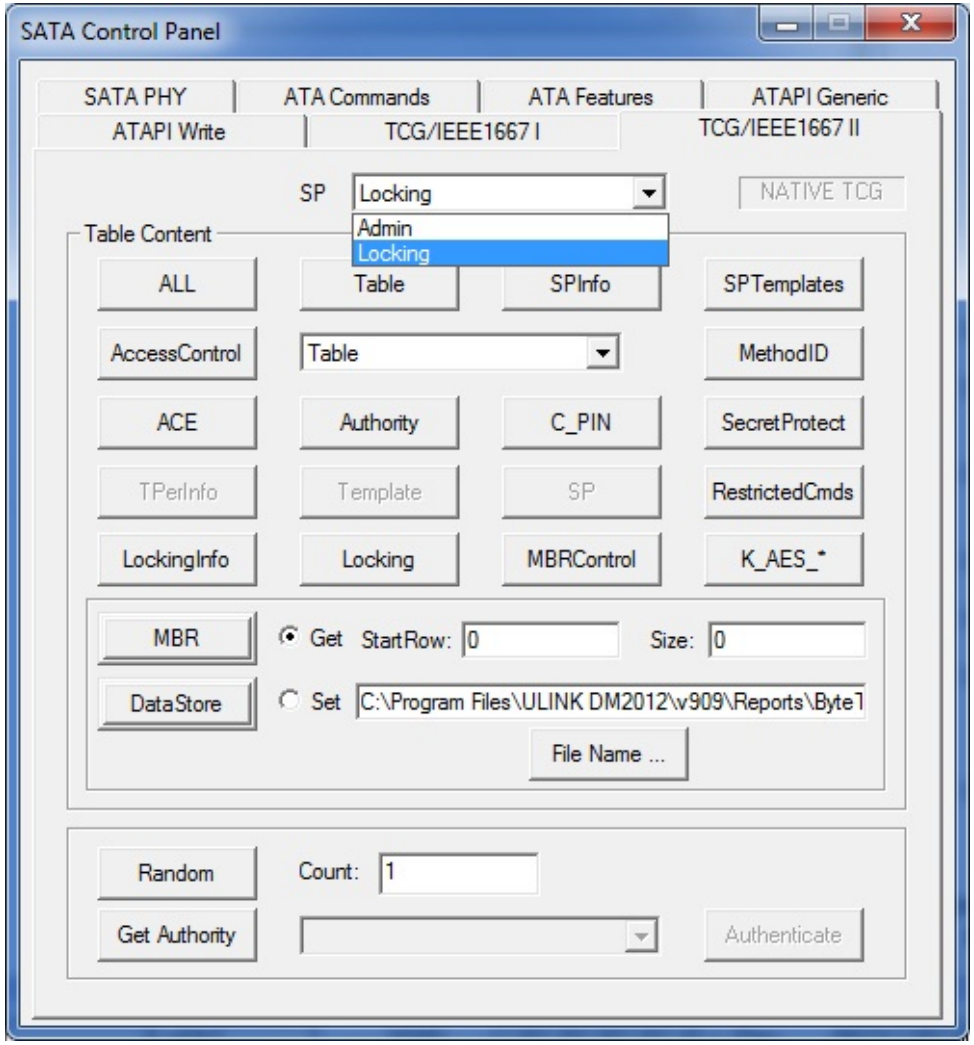

# THANK YOU!

# DriveMaster ControlPanel GUI




- GUI Functions
- Device Capabilities
- Level 0 Discovery
- COMID/MSID
- K_AES/PSID Support
- Stack/TPer Reset
- Get/Set Properties
- Activate/Revert/RevertSP
- Get Current State
- IEEE1667 Probe
- IEEE1667 TCG Get Silo Capabilities

# DriveMaster ControlPanel GUI (Cont.)




GUI Functions (Cont.)

**Table Contents**

- AdminSP/LockingSP
- ALL Object Tables over SP
- Individual Table

**Get/Set Byte Table**

- MBR Byte Table
- DataStore Byte Table

**Methods**

- Random
- Authenticate

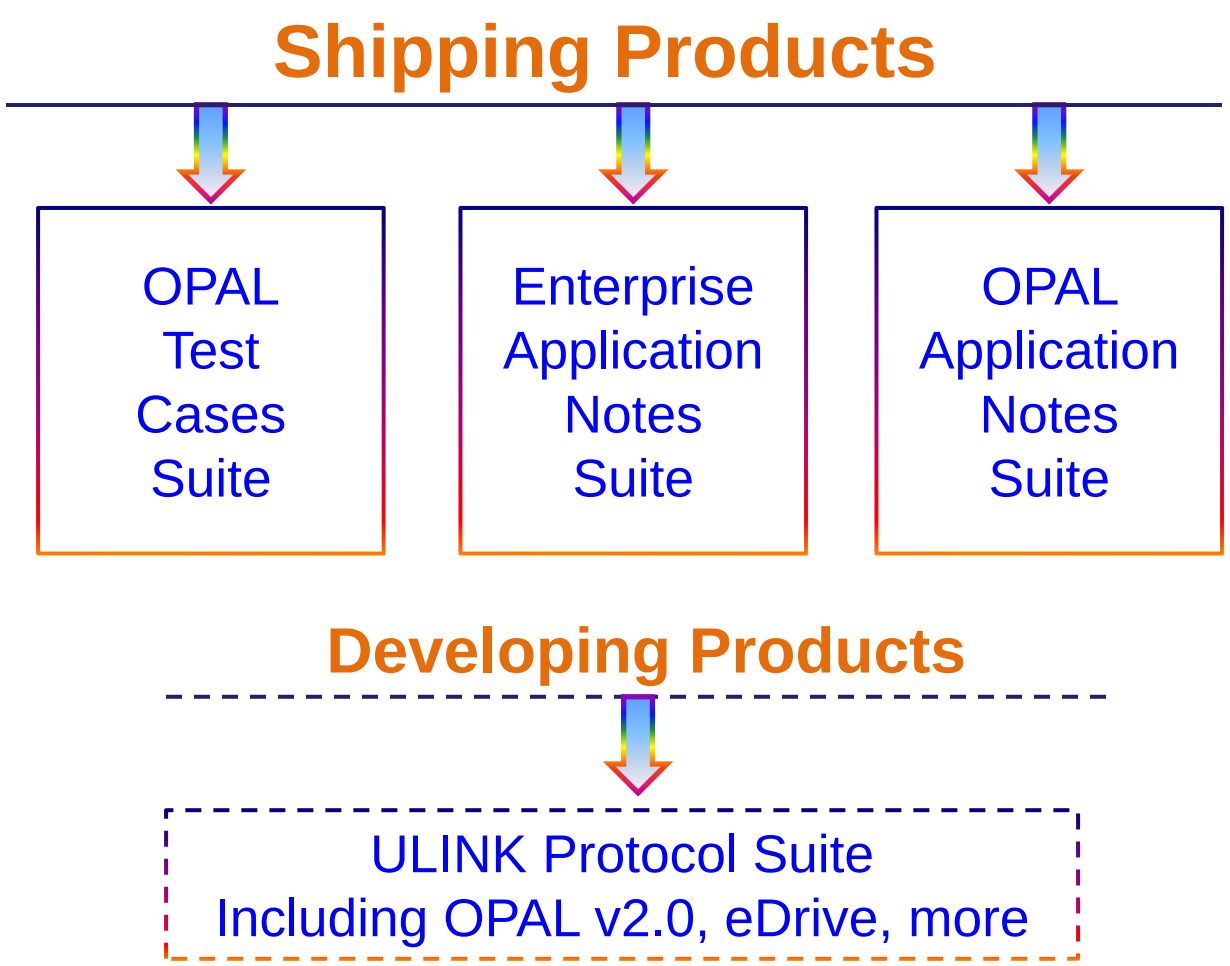
# OPAL & IEEE 1667 Command List

- Security Protocol 1 – Generic
  - LEVEL 0 DISCOVERY
  - PROPERTIES
  - START SESSION
  - SYNC SESSION
  - START TRUSTED SESSION/
  - SYNC TRUSTED SESSION
  - ENDSESSION/CLOSESESSION
  - GET ACL
  - NEXT
  - AUTHENTICATE
  - GENKEY
  - GET
  - SET
  - START TRANSACTION
  - END TRANSACTION
- Security Protocol 1 – FeatureSet Specific
  - ACTIVATE/REACTIVATE (OPAL)
  - REVERT/REVERTSP (OPAL)
  - ERASE (ENT/OPAL FeatureSet)
  - RANDOM (ENT/OPAL v2.0)
- Security Protocol 2
  - GET_COMID
  - HANDLE_COMID_REQUEST
  - GET_COMID_RESPONSE
  - VERIFY_COMID_VALID
  - STACK_RESET/TPER_RESEST
- IEEE1667 - Security Protocol 0xEE
  - PROBE Silo
  - TCG Silo
    - Get Silo Capabilities
    - Transfer/Get Transfer Result
    - Stack Reset/TPer Reset


# DriveMaster OPAL Command Examples

| DriveMaster Commands | Purposes | Examples | Comments |
|---|---|---|---|
| TCG_Discovery | Get Level 0 Discovery Information | *TCG_Discovery* | |
| TCG_SetHostProperties<br>TCG_GetTPerProperties | Set Host Property<br>Get Host&TPer Properties | *TCG_SetHostProperties*<br>*TCG_GetTPerProperties* | |
| TCG_StartSession<br>TCG_SyncSession | Start Session<br>Sync Session | *TCG_StartSession 1, 0000020500000001h, 1* | HostSID = 1, SPUID = Admin SP, Write = 1 |
| TCG_HostEndSession<br>TCG_TPerEndSession | End Session | *TCG_HostEndSession*<br>*TCG_TPerEndSession* | |
| TCG_Get_Rqs<br>TCG_Get_Rsp | Fetch the values of selected table cells | *TCG_Get_Rqs*<br>*TCG_Get_Rsp 1,v0* | Define the scope of the data to be retrieved |
| TCG_Set_Rqs<br>TCG_Set_Rsp | Change the values of selected table cells | *TCG_Set_Req*<br>*TCG_Set_Rsp* | Define location and values to be changed |
| TCG_Activate_Rqs<br>TCG_Activate_Rsp | Manage the life cycle of manufactured SPs | *TCG_Activate_Rqs*<br>*0000020500000002h*<br>*TCG_Activate_Rsp* | SPUID = LockingSP |

# ULINK Test Suites



# TCG SWG OPAL Test Case

## Section A: Basic Grammar - Generic

| Test Cases | ULINK Test Scripts |
|---|---|
| A0: Identify Device | IdentifyDevice |
| A1: Trusted Send/Receive | TCGSend_Recv |
| A2: Protocol ID = 0 related | ProtocolID_0 |
| A3: Level 0 Discovery | Discovery0 |
| A4: Synchronous Communication Protocol | SynchroPtc |
| A5: ComPacket/Packet/SubPacket | ComSubPacket |
| A7: Transaction | Transaction |
| A8: Ending Session | EndSession |
| A9: Empty Atom | EmptyAtom |
| A10: Properties | PropertiesSet<br>PropertiesGet |
| A11: Start/SyncSession() | StartSyncSession<br>StartSyncSession_OptParams |

## Section A: Basic Grammar - Method

| Test Cases | ULINK Test Scripts |
|---|---|
| A6: Method invocation/response | Method_RegSession<br>Method_CtrlSession |
| A12: Get() | Get_Byte_GramChk<br>Get_ObjAdminSP_GramChk |
| A13: Set() | Set_Byte_GramChk<br>Set_ObjLKSP_GramChk |
| A14: Next() | Next_AdminSP_GramChk |
| A15: GetACL() | GetACL_AdminSP_GramChk |
| A19: RevertSP() | RevertSP_GramChk |

## Section C: Table Contents

| Test Cases | ULINK Test Scripts |
|---|---|
| C1: Level 0 Discovery contents | DiscoveryTable |
| C2: Properties() contents | PropertiesTable |
| C3: Get() contents | Get_ByteTable_All<br>Get_ObjTable_AdminSP_All<br>Get_ObjTable_LockSP_All |
| C4: Next() contents | Next_Table_AdminSP<br>Next_Table_LockSP |
| C5: GetACL() contents | GetACL_Table_AdminSP_All<br>GetACL_Table_LockSP_All |

## Section D: Grammar and Effect

| Test Cases | ULINK Test Scripts |
|---|---|
| D1: ACE.Set() | ACESet |
| D2: Authority.Set() | AuthoritySet |
| D3: C_PIN.Set() | C_PinSet |
| D4: Locking.Set() | LockingSet_RangeStartLength<br>LockingSet_ReadLock / LockingSet_WriteLock |
| D5: MBRControl.Set() | MBRControlSet |
| D6: MBR.Set() | MBRSet |
| D7: DataStore.Set() | DataStoreSet |
| D8: K_AES_*.GenKey() | GenKey_Effect |
| D9: Activate() | Activate_Effect |
| D10: Revert()/RevertSP() | Revert_AdminSP_Effect<br>Revert_LockSP_Effect / RevertSP_Effect<br>Act_Revert_RstrCmds |
| D11: Power Cycle | PowerCycle |