Flash Memory Summit

Enhancing Data Protection with Advanced Security Features of PBSSD

Presenter: Sung Kyu Park (Principal Engineer @ Samsung Electronics)

AGENDA

- PBSSD Introduction

- PBSSD's Advanced Security Features
  - Data-at-rest Encryption using SED SSDs ※ SED: Self Encrypting Drive
  - SSD Authentication using SPDM ※ SPDM: Security Protocol and Data Model
  - Ransomware Detection using NVMe CMDs

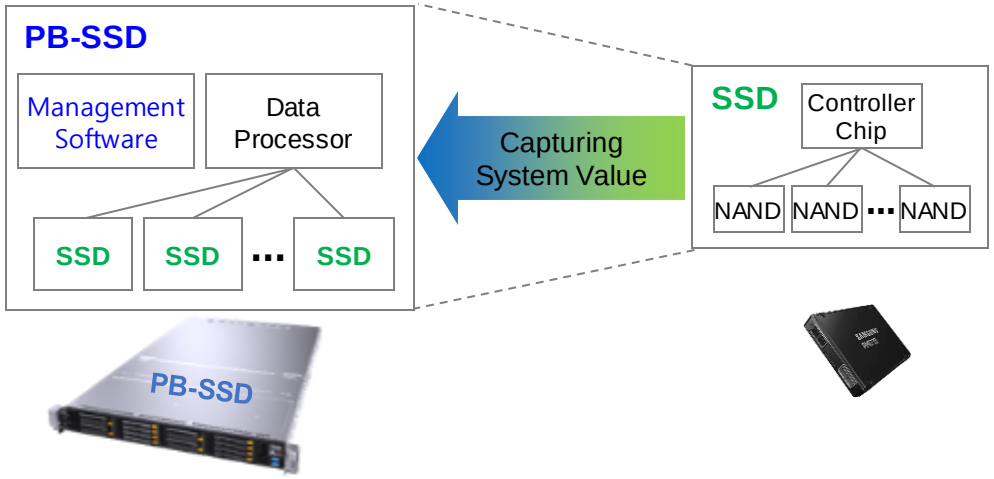
- Conclusion

PBSSD (Petabyte SSD) Concept

- Capturing more value by moving up to the next level: SSD array box from single SSD
  - PBSSD is an ultra-dense storage which expands Samsung's SSD technology to the storage box level
  - PBSSD provides high bandwidth/efficiency/capacity than simple combination of CPU and SSDs

PB-SSD =
SSDs + **box-level value***

* IO controller +
box-level optimization for
performance/power/endurance



(normal) SSD =
NAND chips + **drive-level value***

* IO controller +
device-level optimization for
performance/power/endurance

PBSSD Hardware Architecture

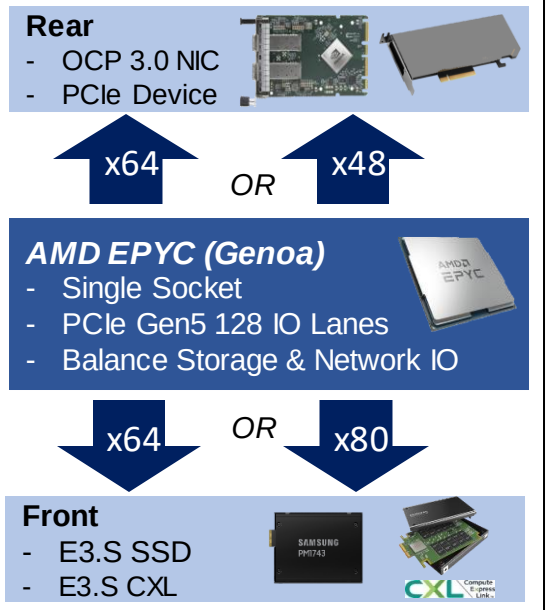
- Provide high performance & massive storage with PCIe Gen5, E3.S F/F, and NVMe-oF
  - Co-design & co-develop PBSSD HW with SMC

Petabyte Scale Massive Storage

32x E3.S 1T SSD(x2)

Ultra High Performance Storage

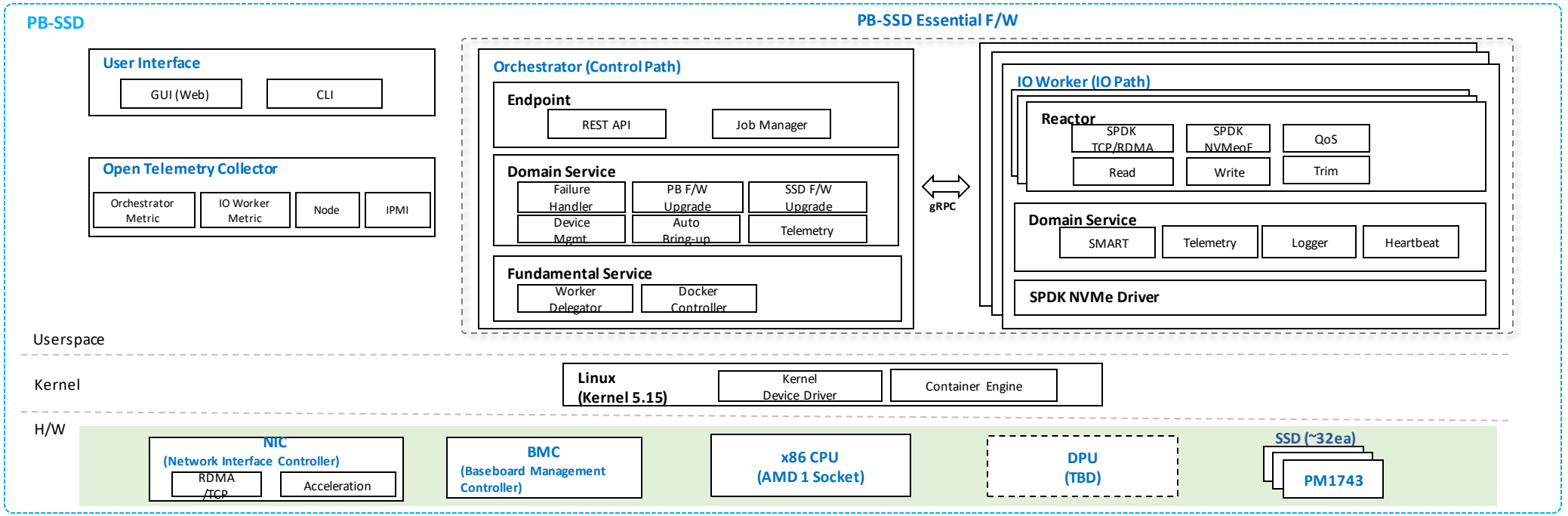
16x E3.S 1T SSD (x4)



CPU	1 x 32-core AMD Genoa Processor (32 threads)	
Main Memory	4 x Samsung DDR5 32GB	
I/O Modules	1 x IO Module	
I/O Connectivity	2 x NIC (2 x 100Gb ports per NIC)	
Management	1 x NIC (1 x 1GbE port per NIC)	
Form Factor	2U	1U
Flash Storage	Samsung PM1743 SSD (15.86TB) x 32ea	Samsung PM1743 SSD (15.86TB) x 16ea
PCI Express	5.0	
Weight	TBD	
Power Supplies	2000W (Titanium level, 80%) Redundant Supply	

PBSSD Firmware Architecture

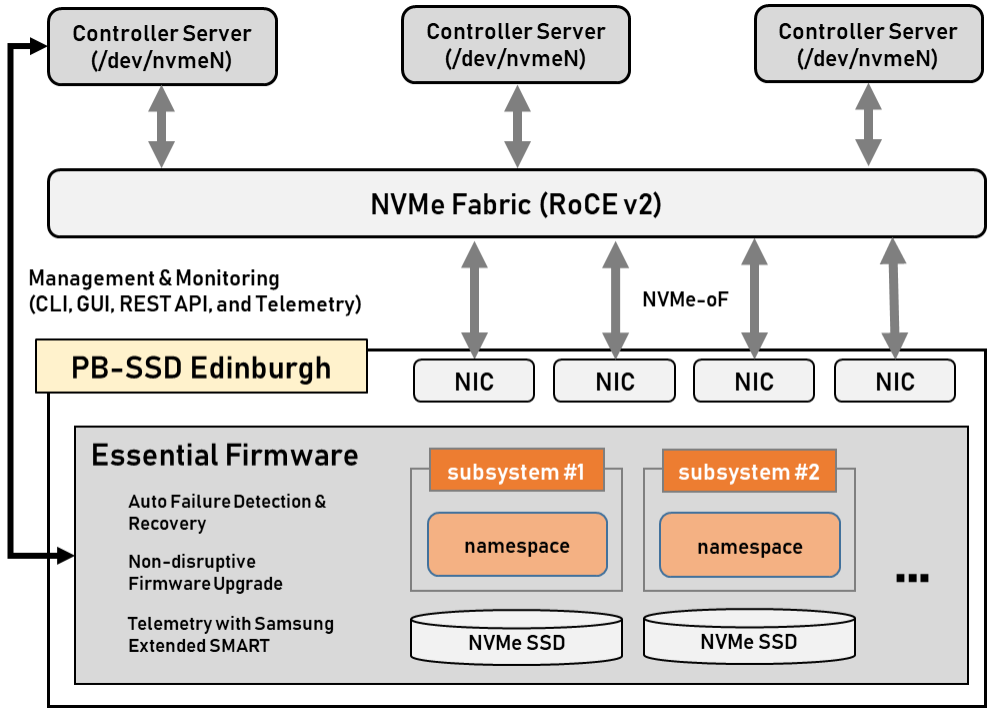
- PBSSD firmware is designed for scalability, serviceability, and availability



PBSSD: Fabric-attached JBOF w/ Samsung's SSD Technology

- High Performance with Power-efficiency
  - Static/dynamic power management

- To save OPEX by high RAS, PBSSD offers management features,
  - Auto failure detection & recovery
  - Non-disruptive firmware upgrade
  - SSD anomaly detection w/ Samsung Extended SMART
  - Security



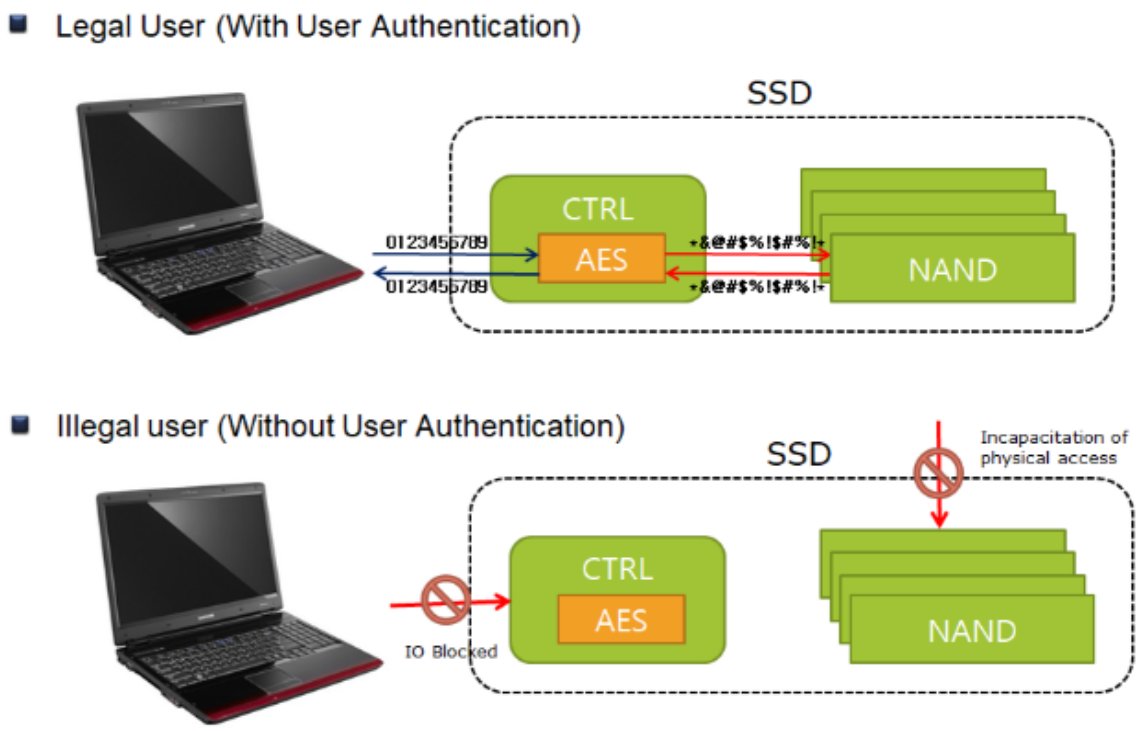
Flash Memory Summit

PBSSD's Advanced Security Features

- Data-at-rest Encryption using SED SSDs
- SSD Authentication using SPDM
- Ransomware Detection using NVMe CMDs

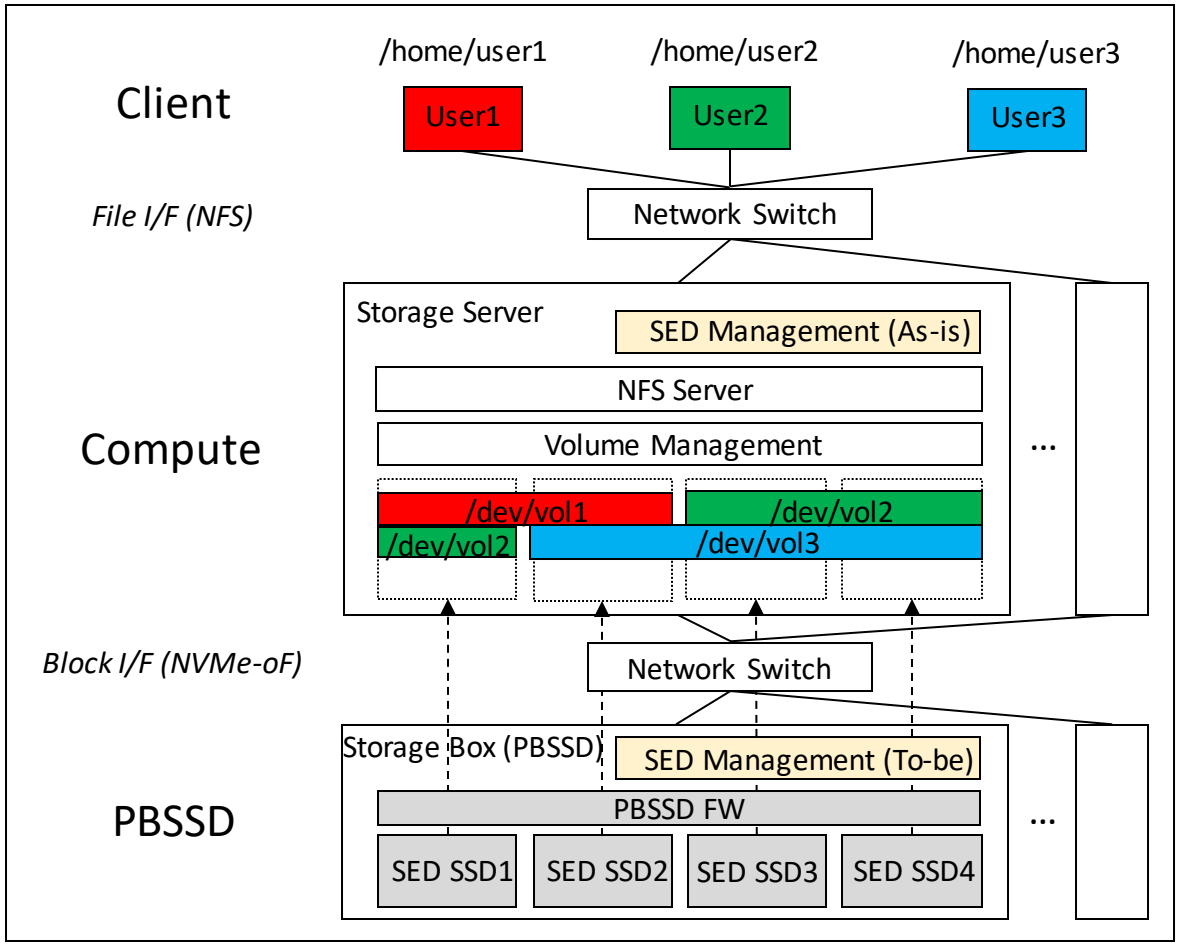
SED (Self Encrypting Drive)

- A storage with security feature which provides HW-based data encryption
  ※ AES Engine
- Without authentication, data access is not possible
  - SED authentication process is executed when the device is power-on
  - If the authentication process is successful, the device remains unlocked until power-off



SED Management

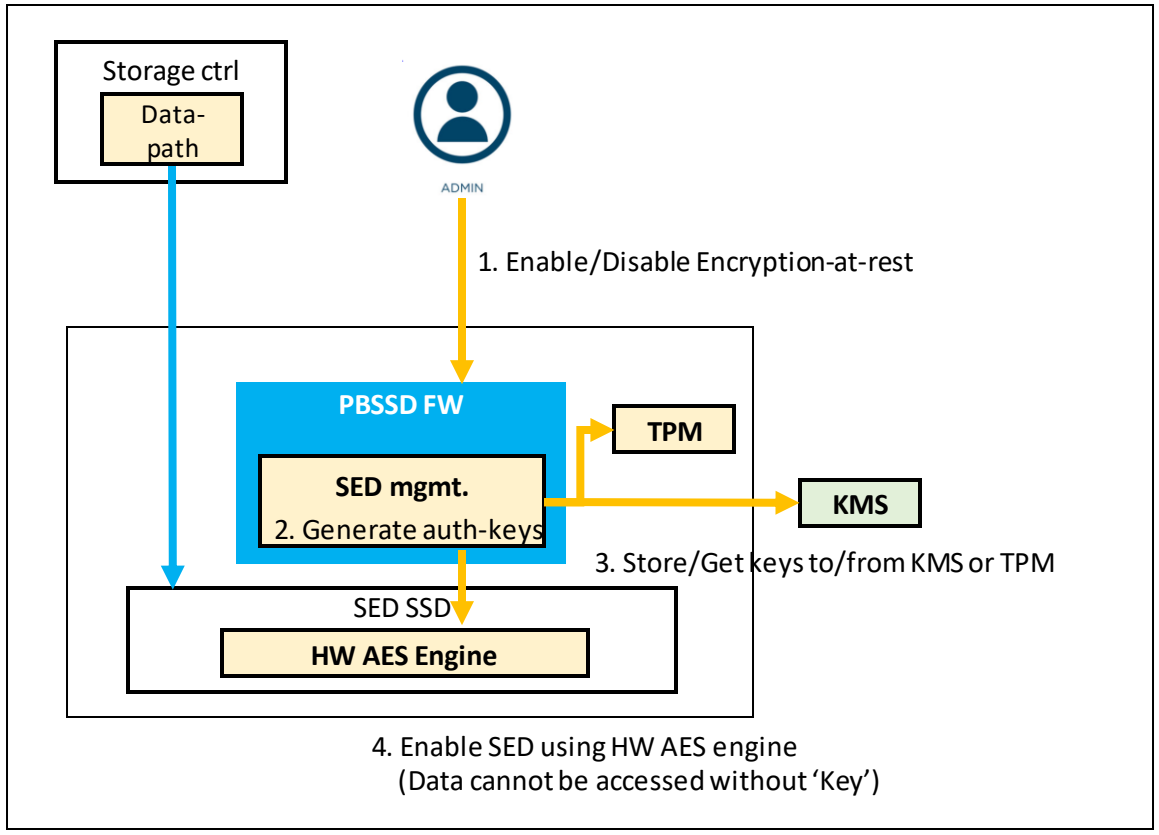
- As-is
  - SED management had to be performed in the compute server
- To-be
  - Perform SED management in PBSSD, thus reducing the overhead in compute server
    - Can be combined with customer's SW-based encryption
    - No performance degradation due to HW-based operation



SED Management @ PBSSD

- Provide the data-at-rest encryption using SED SSDs, which supports full-disk encryption (FDE) of data

- SED management @ PBSSD
  - Generate authentication keys for SED SSDs using cryptographic library
  - Manage authentication keys with onboard (TPM) or external key management (KMS)



SED Management @ PBSSD

- Init
  - Enable SED feature for PBSSD
- List
  - List all SSD status in PBSSD
- Revert
  - Disable SED feature with/without erasing data
- Unlock
  - Unlock SSD in PBSSD for Read/Write

```
psd@R2U22-PSD-4-PB-Target:~/petaos_noerase$ sudo ./bin/poseidonos-cli opal
Error: requires at least 1 arg(s), only received 0
Usage:
  poseidonos-cli opal [flags]
  poseidonos-cli opal [command]

Available Commands:
  init          Init sed command on certain controller.
  list          List all controllers in the system.
  revert        Revert sed command on certain controller.
  revertnoerase Revert sed command on certain controller without erasing data.
  unlock        Unlock certain controller.
```

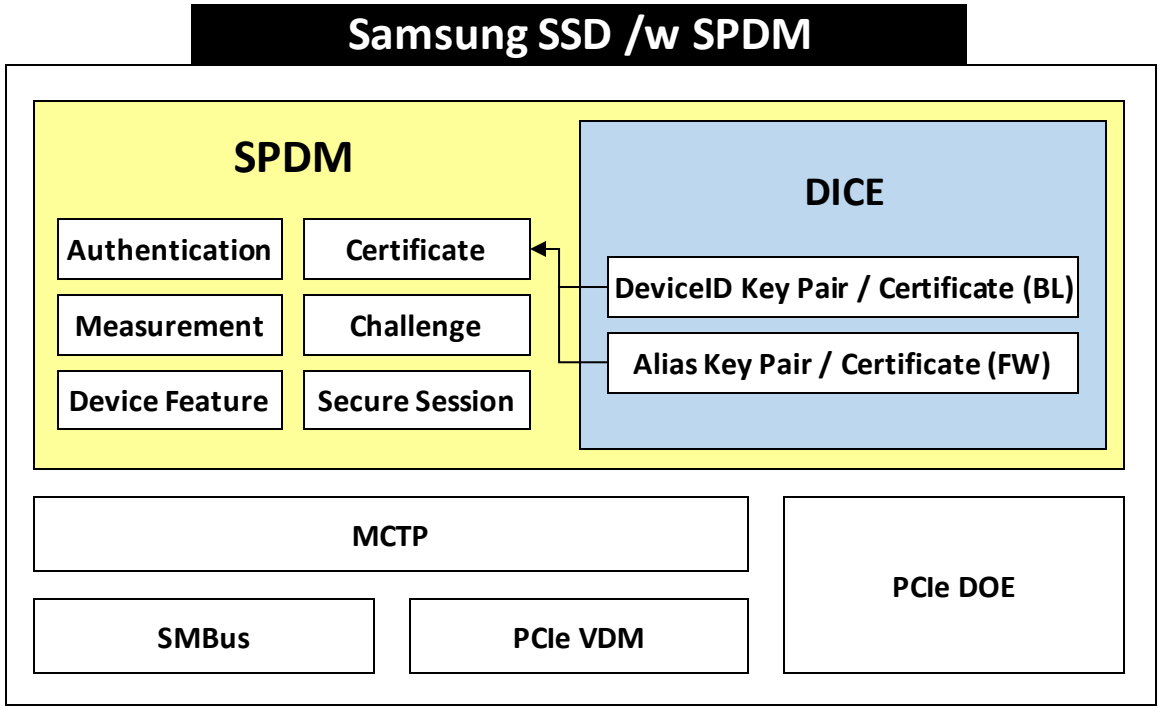
```
psd@R2U22-PSD-4-PB-Target:~/petaos_noerase$ sudo ./bin/poseidonos-cli opal init -c 0000:4d:00.0
 (0) - Success
Cause: NONE
Solution: NONE
psd@R2U22-PSD-4-PB-Target:~/petaos_noerase$ sudo ./bin/poseidonos-cli opal list
Address        |Name          |Serial              |Locked |LockingEnabled |LockingSupported
-------------- |------------- |------------------  |------ |-------------- |--------------
0000:4d:00.0   |unvme-ns-0    |000050M100001       |false  |true           |true
0000:4e:00.0   |unvme-ns-1    |000050M100002       |false  |false          |true
0000:4f:00.0   |unvme-ns-2    |000050M100003       |false  |false          |true
0000:50:00.0   |unvme-ns-3    |000050M100004       |false  |false          |true
0000:51:00.0   |unvme-ns-4    |000050M100005       |false  |false          |true
```

```
psd@R2U22-PSD-4-PB-Target:~/petaos_noerase$ sudo ./bin/poseidonos-cli opal revert -c 0000:4d:00.0
 (0) - Success
Cause: NONE
Solution: NONE
psd@R2U22-PSD-4-PB-Target:~/petaos_noerase$ sudo ./bin/poseidonos-cli opal list
Address        |Name          |Serial              |Locked |LockingEnabled |LockingSupported
-------------- |------------- |------------------  |------ |-------------- |--------------
0000:4d:00.0   |unvme-ns-0    |000050M100001       |false  |false          |true
0000:4e:00.0   |unvme-ns-1    |000050M100002       |false  |false          |true
0000:4f:00.0   |unvme-ns-2    |000050M100003       |false  |false          |true
0000:50:00.0   |unvme-ns-3    |000050M100004       |false  |false          |true
0000:51:00.0   |unvme-ns-4    |000050M100005       |false  |false          |true
```

SPDM (Security Protocol and Data Model)

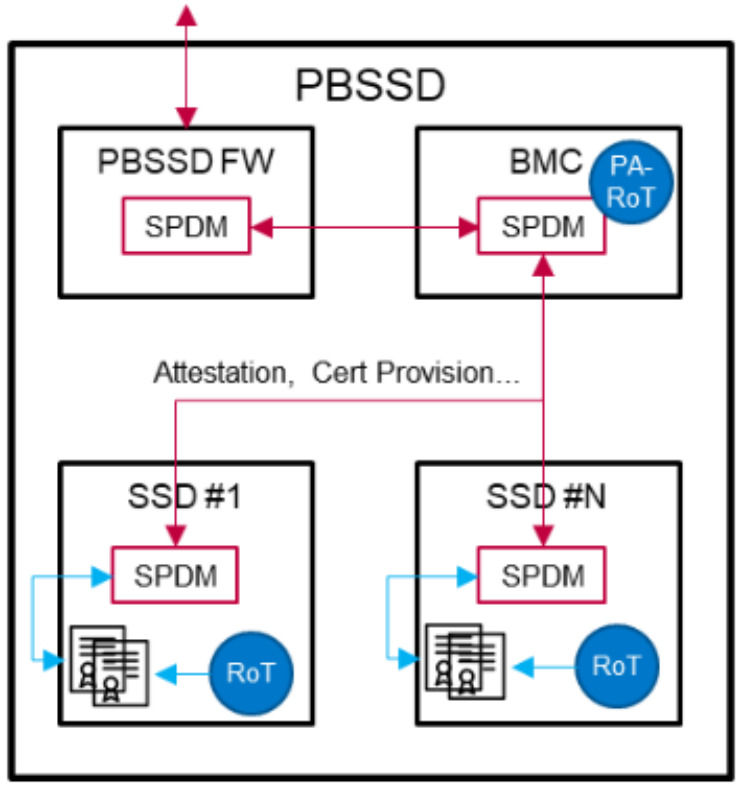
- Enable authentication, attestation and key exchange to assist in providing infrastructure security enablement

- SPDM Specification Configuration
  - SPDM: attestation protocol spec.
  - DICE: spec. for key generation of each layer
  - MCTP/DOE: transport protocol spec.



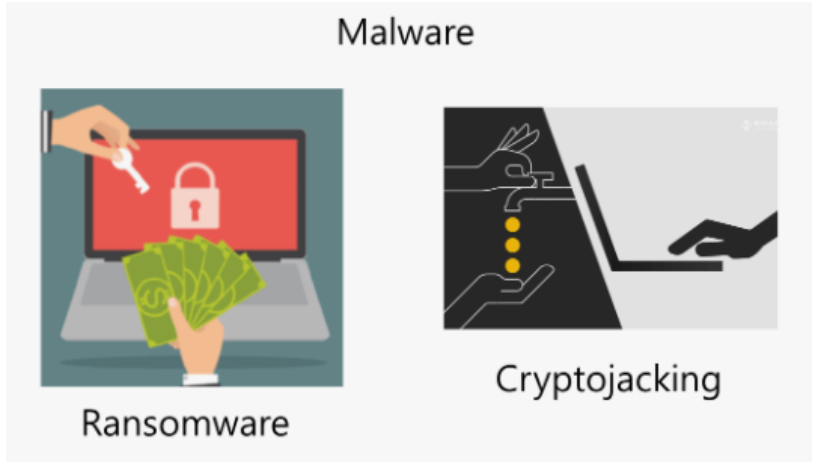
SSD Authentication using SPDM @ PBSSD

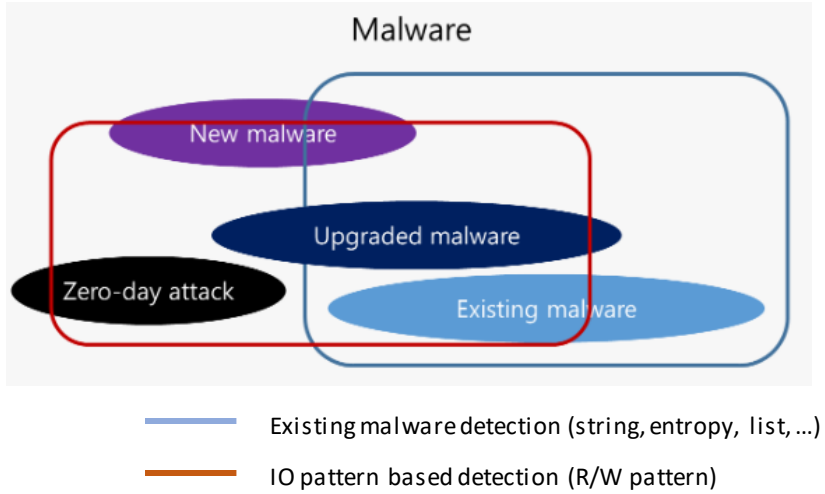
- Attestation
  - SSD: transmit the digital signature for the certificate chain and device measurement (code & configuration hash)
  - PBSSD FW: verify the identity authentication and device measurement of the target device
    - Identity authentication: Ensure the SSD has not been replaced
    - Firmware measurement: Ensure that SSD FW status is normal
- PBSSD can provide SSDs that measure the normal state to the customer through the SPDM's Attestation



Ransomware Trend

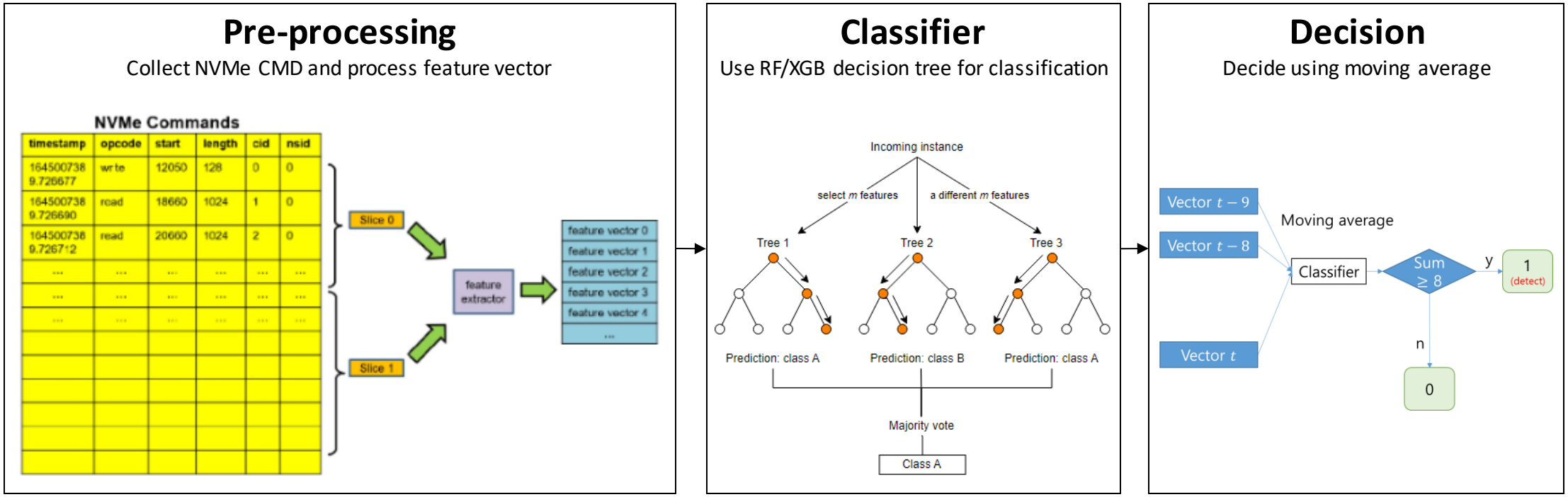
- Limitation in Existing Detection Algorithm
  - Hard to detect ransomware and cryptojacking due to advanced attack level
  - Hard to cope with the new type of malware in the beginning
- Solution
  - Increase the total detection coverage by developing IO pattern based detection algorithm





Ransomware Detection @ PBSSD

- PBSSD can increase ransomware detection coverage in the existing system



Conclusion

- PBSSD is a cutting-edge large-capacity SSD that allows for petabyte-scale storage, providing high performance with power efficiency and TCO reduction

- PBSSD's advanced security features
  - Data-at-rest encryption using SED SSDs
  - SSD Authentication using SPDM
  - Ransomware Detection using NVMe CMDs

Q&A