SDC 19

September 23-26, 2019
Santa Clara, CA

Data-At-Rest Protection at Data Center Scale with NVMe and Opal

Andrzej Jakowski
Adrian Pearson
Intel Corporation

Legal Disclaimer

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel does not control or audit third-party data. You should review this content, consult other sources, and confirm whether referenced data are accurate.

Intel, the Intel logo, and other marks are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Agenda

- Motivations for Data-At-Rest Security
- TCG Opal family for SEDs
- Sedcli – new open source utility for SED management for data center scale (and client)
- Sedcli roadmap
- Call to action

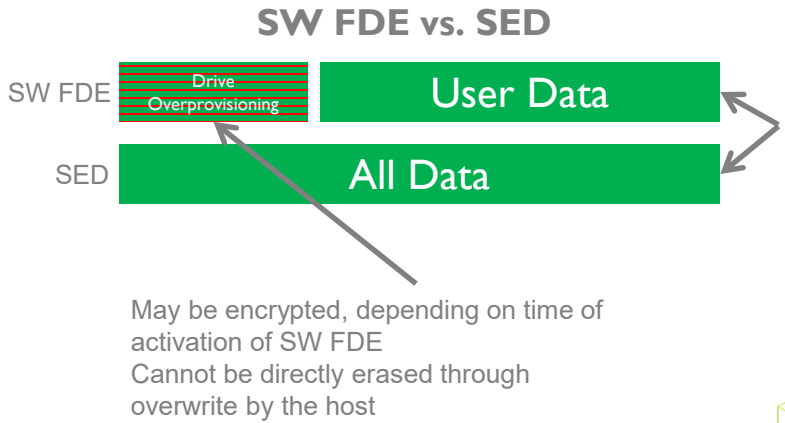
Motivations for Data-at-Rest security

- Data breaches continue to grow in scale and cost to organizations
- Governments are responding by developing new regulations such as the EU GDPR and Lot 9 requirements
- Provisions in these laws discuss topics such as user data rights for data retention, access control, knowledge of who has access to data, etc
- GDPR, in particular, mentions encryption as a path to potential mitigation in the event of data breach.
- Lot 9 requires Secure Data Deletion

https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

Motivations for Data-at-Rest security

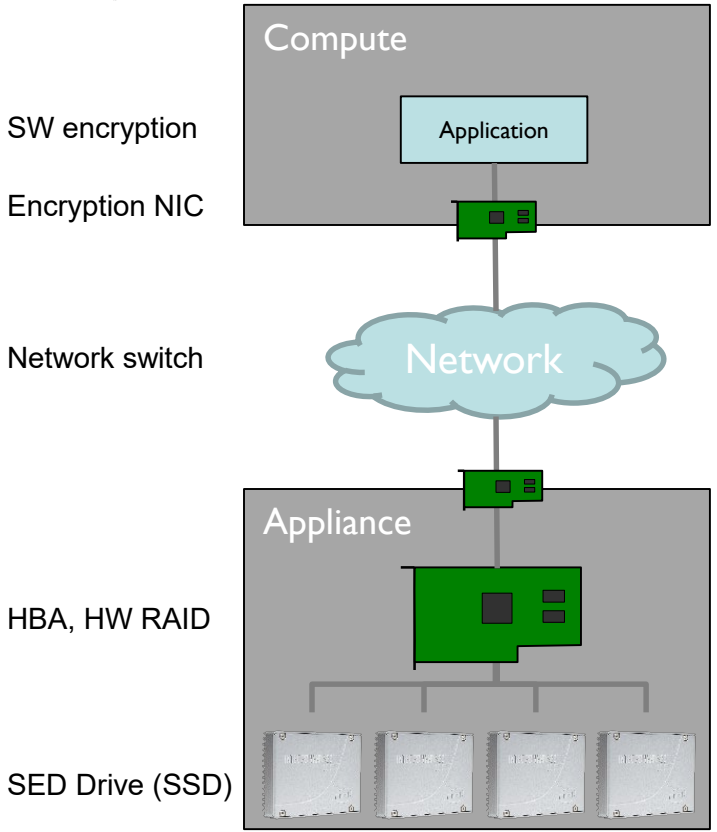
- All user data, regardless of wear leveling, is encrypted as of the first LBA write to the drive
- Data erasure using drive commands ensures erasure of all data – regardless of wear leveling
- SW-FDE does not provide these guarantees
- Increasingly, SED's are deployed to ensure "last mile" compliance and ensure that physical theft does not cause a data breach



Where encryption is done?

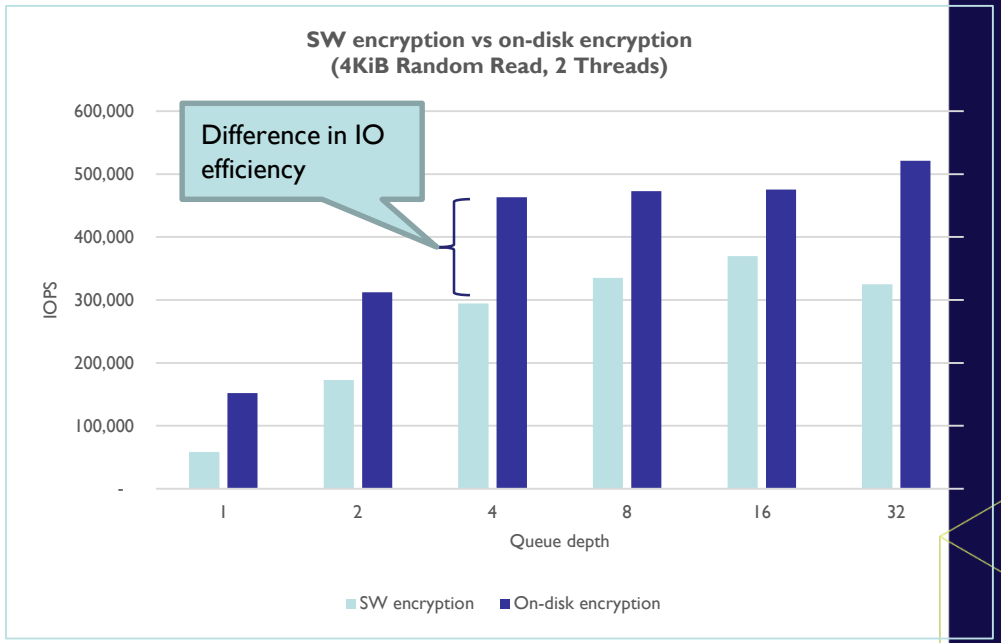
Encryption can be done on different levels. Factors to consider:

- Protection against threat
- Performance impact
- Regulations
- Impact on other processes:
  - Encrypted data may not be compressible



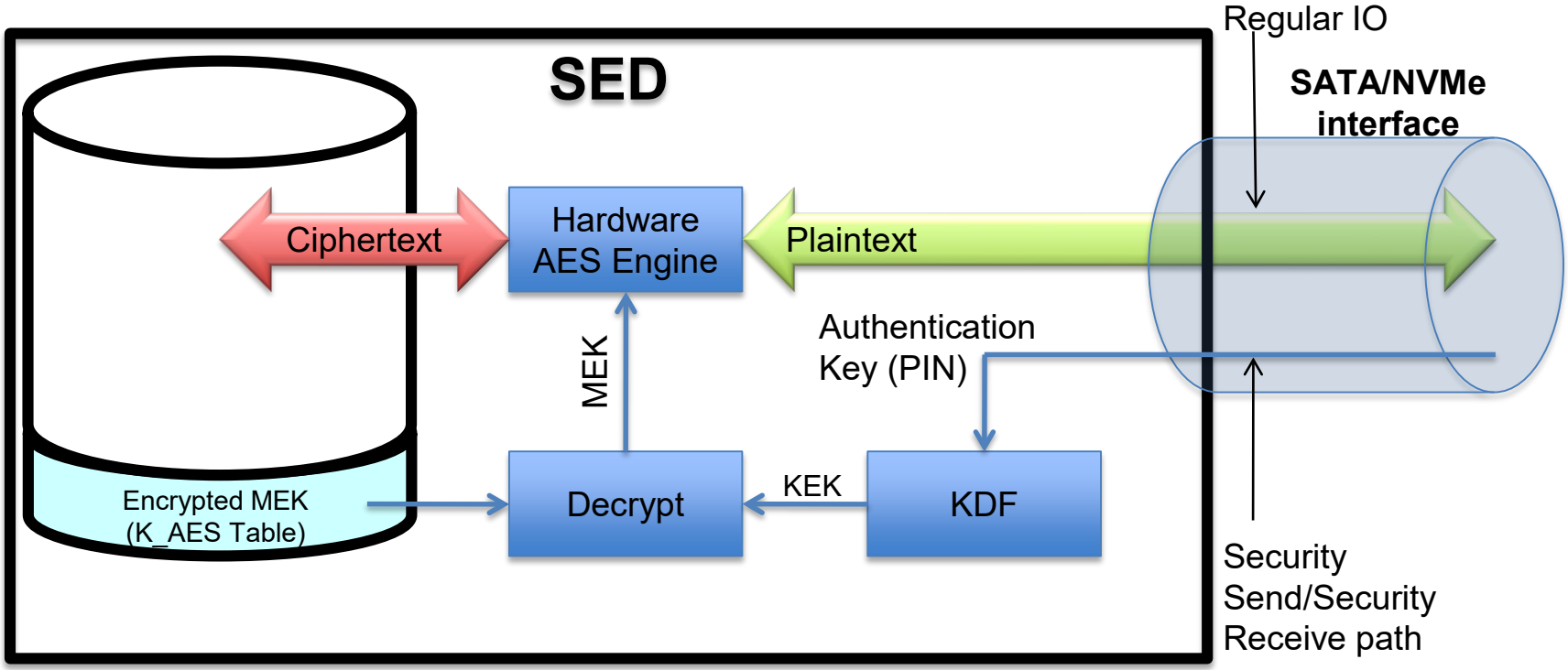
SW encryption versus on-disk encryption

- **SW encryption:**
  - Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) provide near full bandwidth crypto for SW FDE for large transfers
    - However, software overhead remains, adding extra latency – especially for 4K transfers
- **On disk encryption:**
  - SED AES performance provides low latency and bandwidth at interface speeds for all transfer sizes



Source: Intel. System Configuration: Intel ® Xeon Platinum 8200L CPU @ 2.70GHz, DRAM 4GB, Intel DC P4800X 800GB SSD, Debian (Linux 4.9.0-11-amd64 x86_64) with and without SW encryption using LUKS. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks Performance results are based on testing as of 9/17/2019 and may not reflect all publicly available security updates. See configuration disclosure for details. No product or component can be absolutely secure

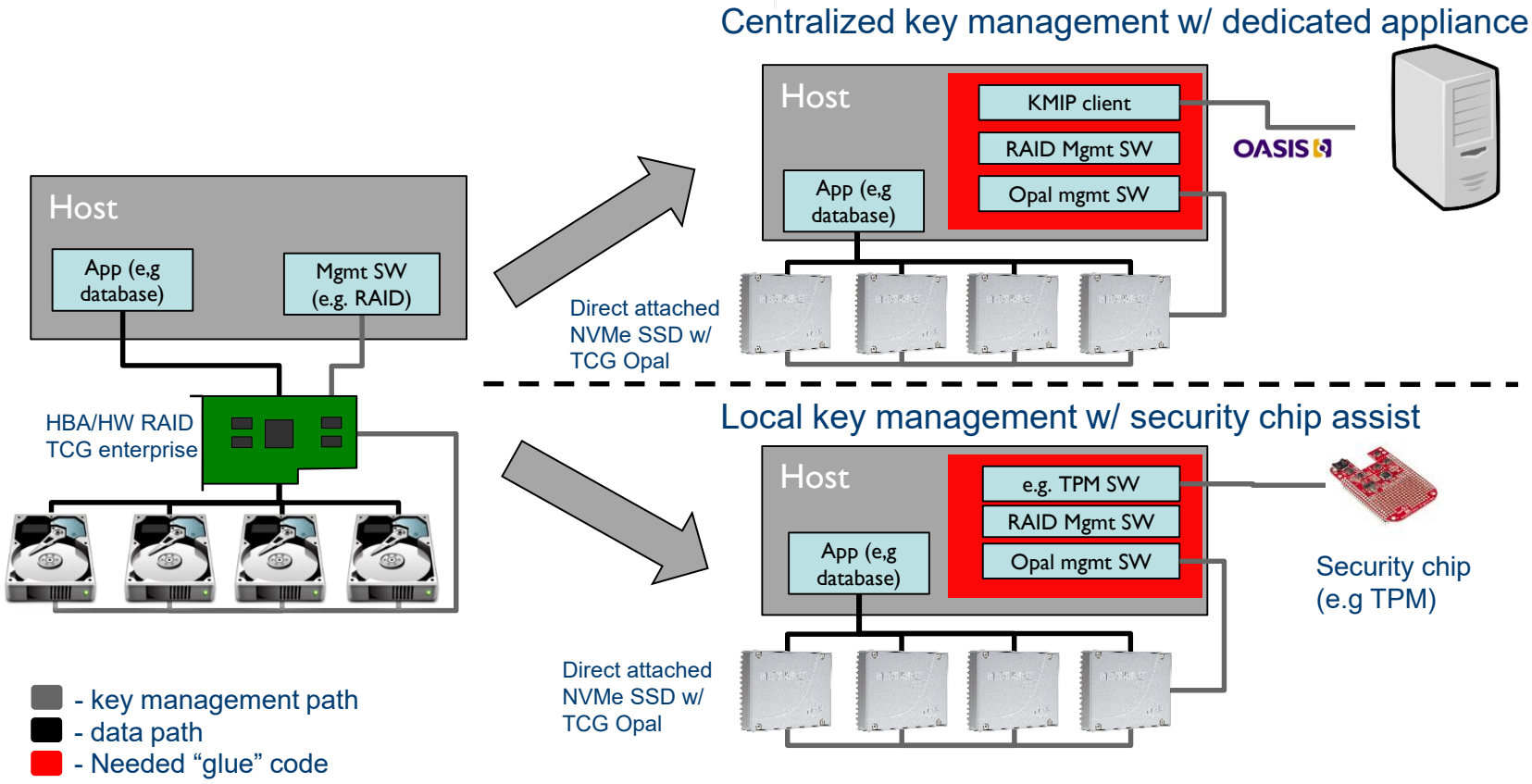
Key management in Opal



Client usages and data center usages are different

- **Client:**
  - Usually requires user to supply key (password) to the disk
  - Pre-Boot-Authentication via Shadow MBR
- **Data center:**
  - Need for automated key management during initial provision and auto unlock on day-to-day operation due to the scale
  - Need for periodic key rotation
  - Need for key backup

Shift to NVMe and the need for new SW tooling



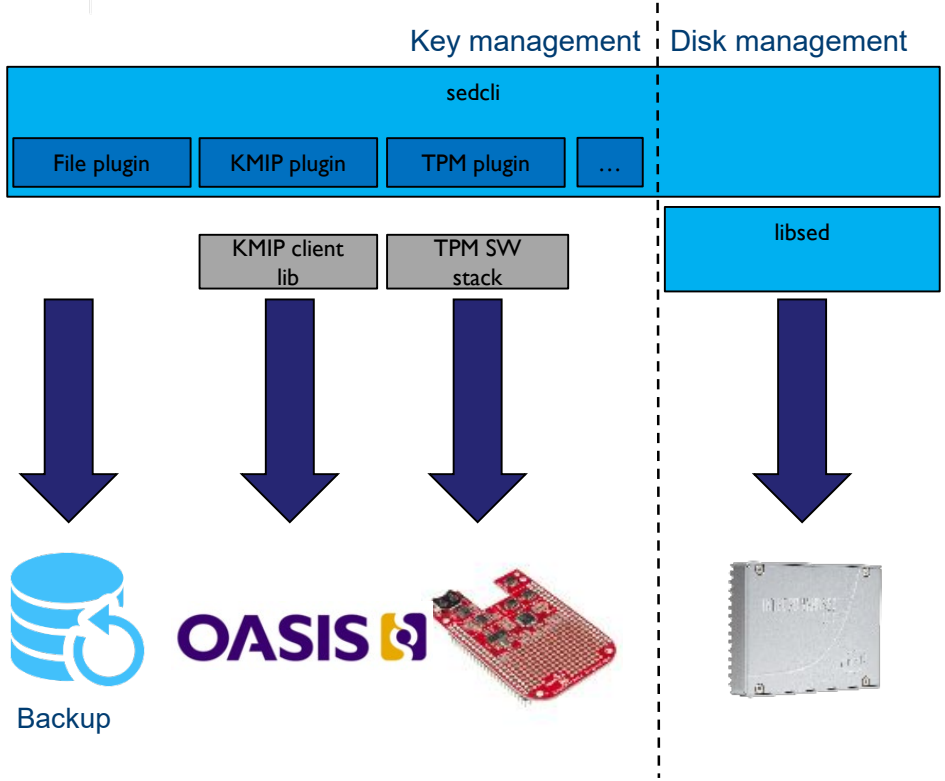
Sedcli SW proposal

Support for data center usages:

- Auto-provision on hot insert or OS boot
- Auto-unlock on hot insert or OS boot
- Support for multiple key managers (OASIS KMIP, TPM)
- Key backup functionality

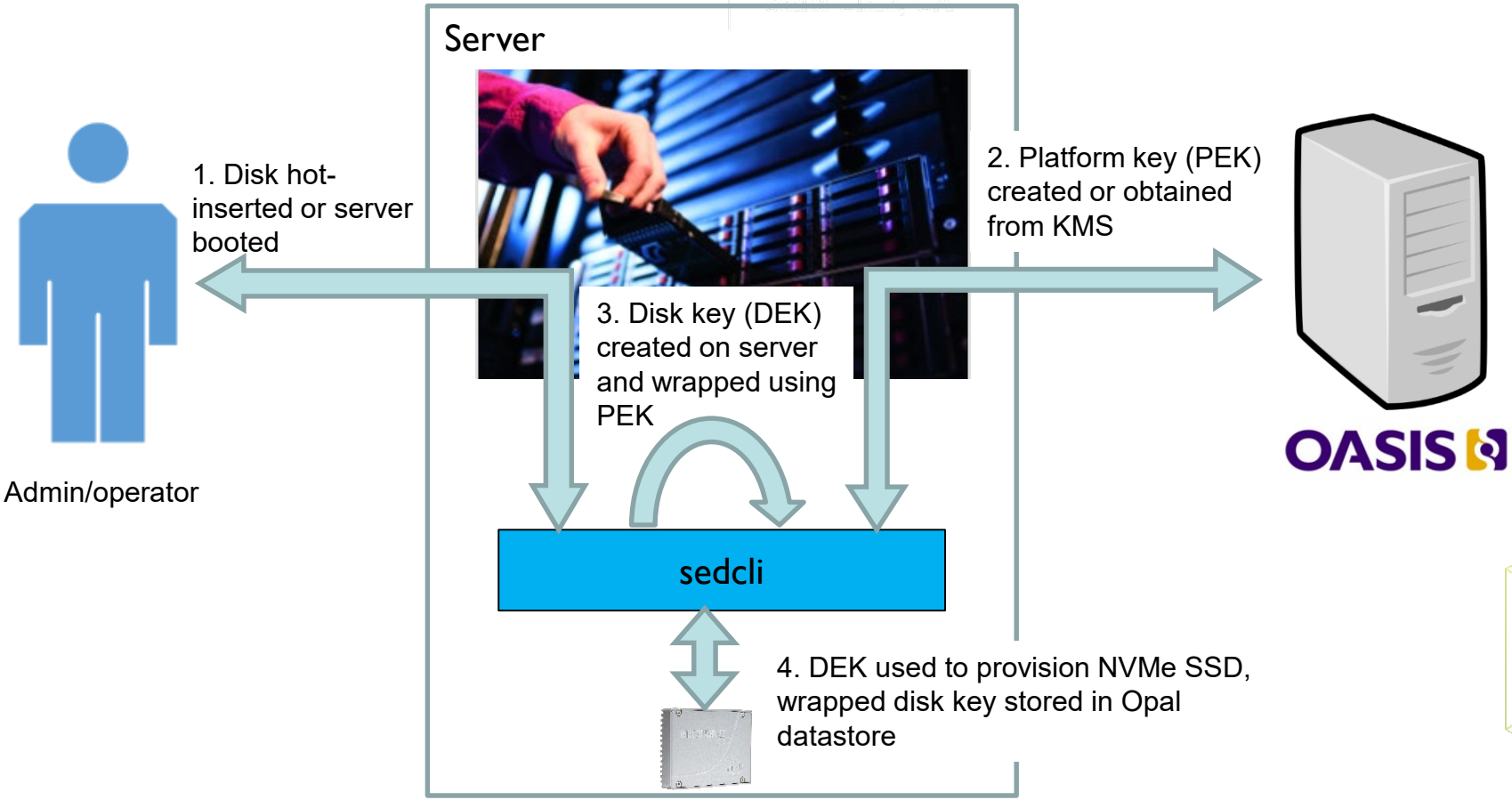
Key SW components:

- Sedcli – modular architecture allowing multiple key managers:
  - OASIS KMIP
  - TPM
- Libsed - enables extensions

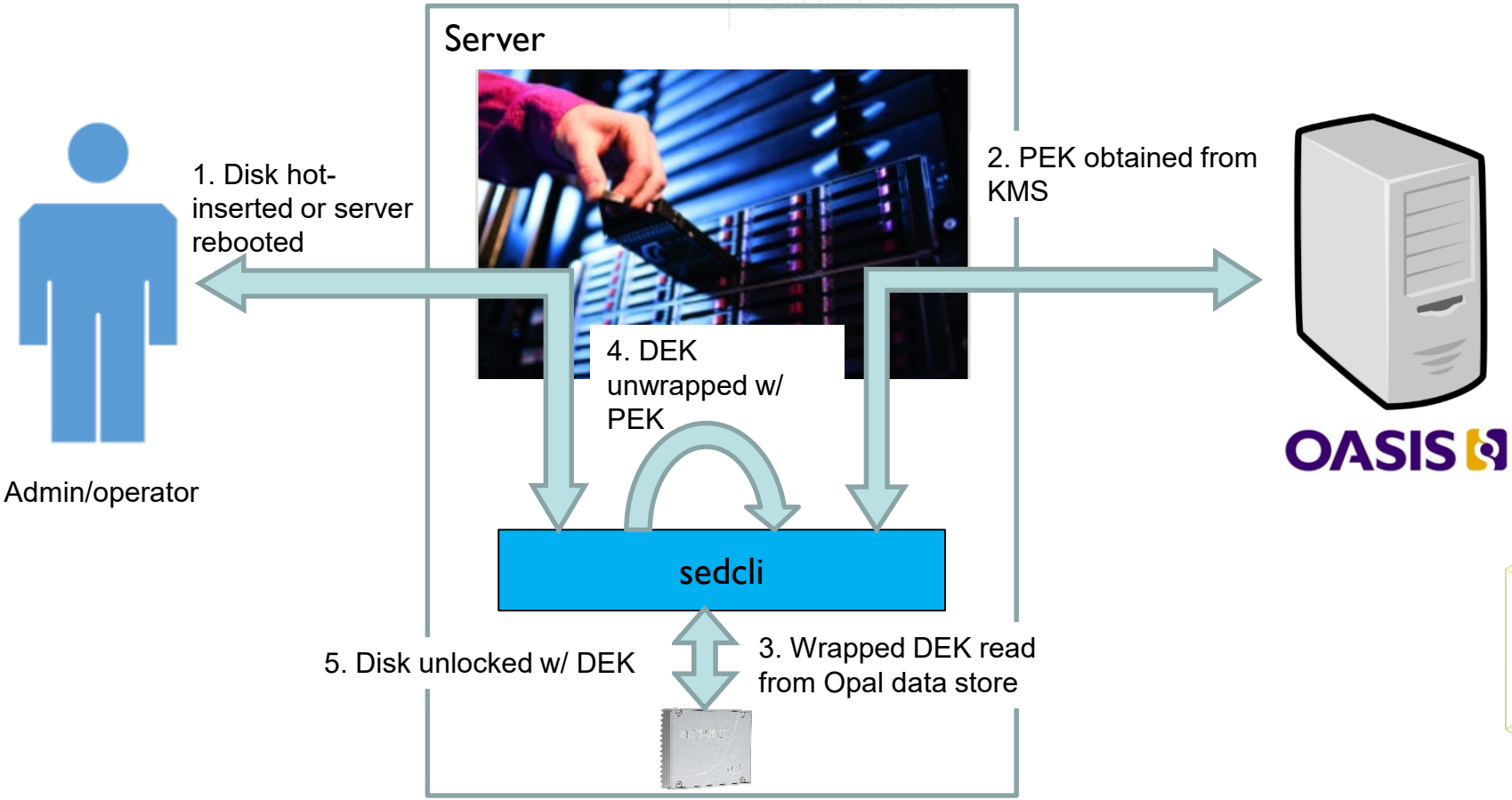


Source code available on https://github.com/sedcli

Envisioned data center auto-provision flow



Envisioned data center auto-unlock flow



Sedcli status and next steps

Client usages:
- Initial provision
- Explicit locking and unlocking
- Changing key for Admin1
- Revert TPER

Data center usages (KMS):
- OASIS KMIP key manager
- Auto initial provision
- Auto unlock
- Key backup

Data center usages (TPM):
- TPM 2.0 based key manager
- Auto initial provision
- Auto unlock
- Key backup

Support for emerging DAR security standards such as NVMe/TCG Key Per IO

Call to action

- Encourage usage and contributions to https://github.com/sedcli
- Provide feedback/additional usage models
- Reach out to us to learn more