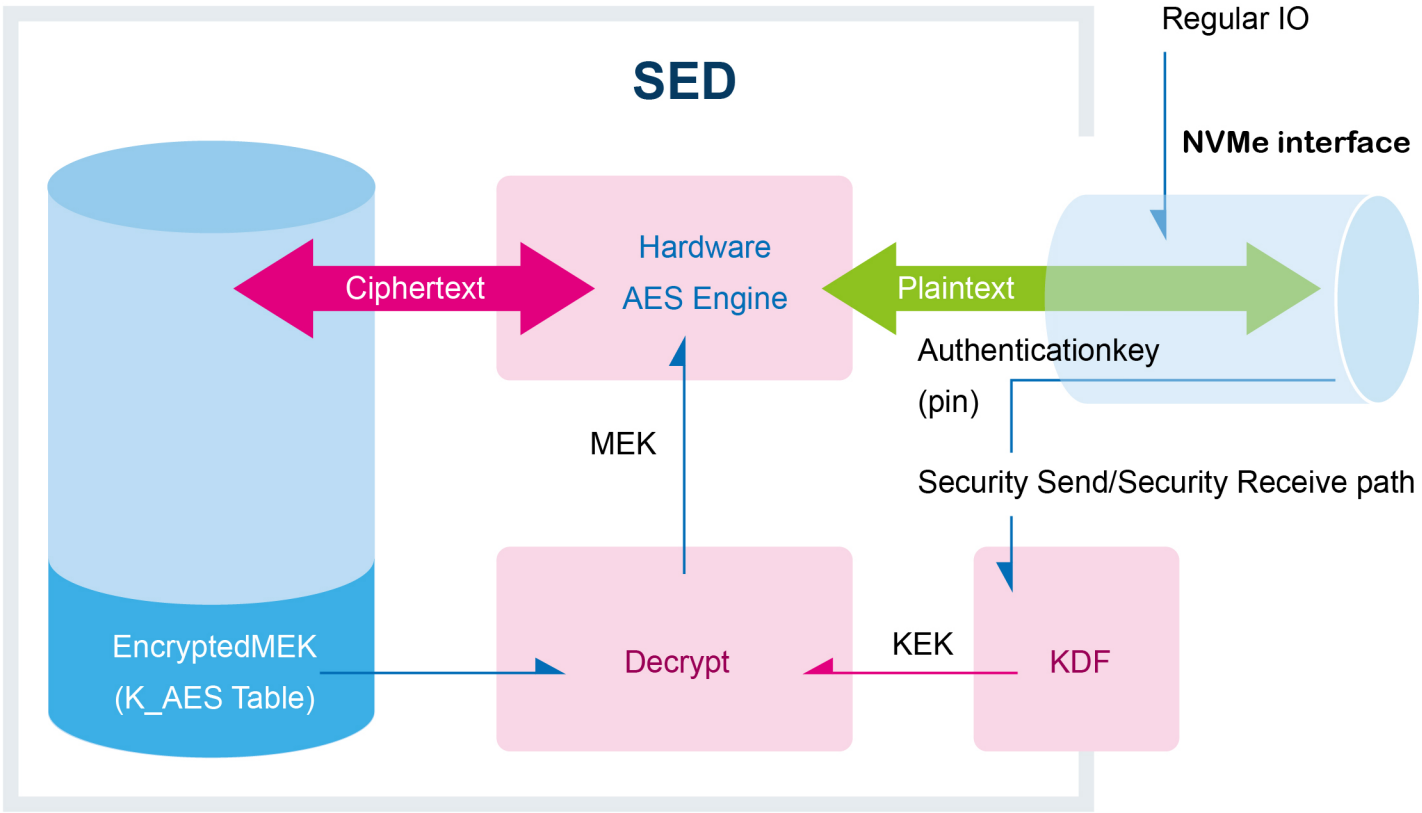
TCG/OPAL 2.0
COMPLIANT SELF-ENCRYPTING DRIVE (SED)

SELF-ENCRYPTING DRIVE (SED)

A Self-Encrypting Drive (SED) is a Storage Device that integrates encryption of user data at rest. All of the user data written to the Storage Device is encrypted by specialized hardware implemented inside the Storage Device Controller. The security and privacy benefits of SEDs are essential in the Internet of Things (IoT), medical devices, industrial systems, retail systems, defense equipment, transportation systems, etc.

All user data written to the SSD is encrypted by specialized hardware implemented inside the SSD controller. The data is decrypted as it is read. The encryption and decryption are performed using a Media Encryption Key (MEK) generated internally inside the SSD. TCG/Opal defines a management interface for a host application to activate, provision, and manage encryption of user data. The specification includes data structures and their required content, as well as mechanisms for managing and configuring Authentication Credentials and access controls. TCG/Opal provides a mechanism by which an Authentication Credential can be set by a host application that manages the TCG/Opal functionality in the SSD, in order to enable control of access to the user data. When an Authentication Credential has been set and the device is locked, it is no longer possible to access the user data. Once the correct Authentication Credential has been supplied to the Storage Device by the host, and the Storage Device is unlocked, data can be read from and written to the device once again.



TCG/OPAL 2.0

TCG/Opal stands for Trusted Computing Group Opal. The Trusted Computing Group is an organization that develops open standards for trusted computing platforms.

The latest Opal Storage Specification is currently available in version 2.0, featuring a demand encryption function for the stored data so that an unauthorized person will not be able to see or access the data, even if possession of a drive was gained.

DRIVE TRUST ALLIANCE

The Drive Trust Alliance brings together the state of the art in SED technology. Storage Device Makers, Storage Security Software Vendors, IT departments, and normal End Users will learn how to employ SED technology to solve many of today's massive and serious data leakage problems.

The Drive Trust Alliance maintains the popular "sedutil" application, which eases configuration of Self-Encrypting Drives implementing the TCG/Opal specification for SATA and NVMe SEDs.

- ### SP OFFERS TCG/OPAL 2.0 COMPLIANT INDUSTRIAL SATA III AND NVME SSDS

  SP Industrial SATA III and NVMe SSDs are equipped with an AES-256 encryption engine, providing hardware-based, secure data encryption, with SED function support and no SSD performance loss. If TCG/Opal features are enabled, the SSDs will follow the TCG/Opal specification and integrate encryption of user data at rest.

  When TCG/Opal features are not enabled, SP Industrial SATA III SSDs can perform alternate data encryption by invoking the ATA security command set encryption features, to provide full-disk encryption (FDE), managed in the host system BIOS. TCG/Opal and ATA security feature sets cannot be enabled simultaneously. The data encryption is always running; however, encryption keys are not managed and the data is not secure until either TCG/Opal or the ATA security feature sets are enabled.

  SP Industrial SATA III and NVMe TCG/Opal Compliant SSDs are fully tested with the Drive Trust Alliance utility program, "sedutil," to confirm compliance with TCG/Opal specification.

  Please contact with SP Sales Representatives to get the latest TCG/Opal 2.0 compliant list.