Media Sanitization and Cryptographic Erase

Organizations such as US Government agencies create, collect, analyze, and retain large amounts of data. All these data sets end up on storage devices that - when decommissioned – may still contain valuable information. The destruction of all data stored on these devices, also known as media sanitization, is governed by multiple standards, e.g., NIST SP800-88 Rev, ISO 27040:2015, and IEEE 2883-2022. They outline how to deploy the different sanitization techniques based on the sensitivity of data stored on the device's media. High-level, these techniques are either non-destructive (device can be reused) or destructive (device is inoperable afterwards). For US Government agencies the national policy for sanitization of devices storing Unclassified to Top Secret data is defined in NSA/CSS Policy Manual 9-12[1]. This policy requires device destructive methods only (Disintegration and Incineration) for sanitization of solid state and hard disk drives. Compare this to the non-destructive methods Clear and Purge, which offer different levels of guarantee that data is unrecoverable. For example, the NVMe[2] Sanitize command has three options (Block Erase, Crypto Erase, and Overwrite), each with different levels of data destruction assurance. Block Erase sanitizes media with a low-level media dependent block erase method; Crypto Erase sanitizes media by destroying the media encryption keys; Overwrite sanitizes media by writing fixed data patterns.

Using Crypto Erase for media sanitization is fast and becoming the preferred technique in many cases, assuming that:

- the storage device supports media encryption technology that meets a minimum set of security requirements. These include e.g., use of approved cryptographic algorithms, proper protection of keys, a given minimum key length, and good quality entropy; and
- the storage devices successfully passed an independent third-party security assessment. These include a FIPS140 Cryptographic Module Validation Program (CMVP) certification and/or a NIAP Common Criteria security evaluation. They provide a certain level of assurance that the cryptography is correctly implemented, keys are properly destroyed or generated, and that basic security requirements are met.

With Cryptographic Erase the device destroys its existing encryption keys and generates new ones. All data encrypted with the destroyed key is no longer recoverable: the key is not available to decrypt any data. Additionally, when data is retrieved from the storage device the data is decrypted using the new key, resulting in an additional level of data scrambling. Encryption key destruction and generation is typically done in about two seconds or less. Most Self-Encrypting Drives support Crypto Erase out-of-the-box.

A Self-Encrypting Drive, or SED, is a storage device with added data security functionality. The device, typically a solid-state drive or hard-disk drive, transparently encrypts all data written to the device and then decrypts it when the data is retrieved from the device. A SED provides data security through data access controls and Crypto Erase, using strong symmetric key encryption for data protection.

---

[1] NSA/CSS POLICY MANUAL 9-12: Storage Device Sanitization and Destruction Manual – Dec. 2020

[2] NVMe or the NVM Express specification defines the interface commands for Non-Volatile Memory devices, such as a Solid-State Drive (SSD).

RPI-CS, Inc.
866.938.7775
6747 Katella Avenue, Cypress, CA 90630

Invoking a Crypto Erase on a SED require host system support and software tools. In some cases, the capability is built into the system (e.g., Dell PERC 11 or a RedData SED CSfC bundle), in other cases the OS or a software tool provides capabilities to invoke a Crypto Erase. These include BitLocker for Windows, Linux distributions with sedutil, manufacturer tools (such as Seagate's SeaTools), software from e.g., Cigent or KLC Group, and the open source SEDutil tool. In other situations, the Crypto Erase capability is part of the physical design and is invoked via e.g., push buttons or ripcords.

Crypto Erase is defined functionality in the Commercial Solutions for Classified (CSfC) Data-at-Rest Capability Package[3]. The Capability Package requires Cryptographic Erase (CE) for reprovisioning of the system, to be triggered after failed authentications, "or as an emergency method of sanitizing the media, in the event proper destruction methods cannot be met." As such, any CSfC solution that implements the Data-at-Rest Capability Package requirements must support CE alongside the dual-layer of encryption (also known as dual-DAR).

In CSfC compliant solutions one layer of encryption (Outer Layer) is typically implemented by a SED with approved Pre-Boot Authentication software, the other layer (Inner Layer) may use software that encrypts individual files or file system volumes. The combined outer and inner layers provide the baseline of a CSfC Dual-DAR solution for data-at-rest security. And both layers must support CE capabilities, typically via software functionality. Different CSfC compliant or approved software packages will provide the required CE capabilities either triggered by policy (e.g., crypto erase data after 10 failed authentications) or invoked by an administrator in case of system reprovisioning.

Invoking a Crypto Erase on a SED that implements the Outer Layer of a CSfC Dual-DAR solution will make the data encrypted by the Inner Layer solution inaccessible. Although this provides a good level of protection against unauthorized data recovery, technically it does not constitute a proper Dual-DAR Crypto Erase. More specifically, there is a requirement that "All DAR FDE components must be cryptographically erased before being provisioned again".[4] This implies that the Inner Layer encryption keys must be destroyed, especially if a copy of that key is stored in another place within the system (e.g., TPM) or outside the system (e.g., a USB-token or key manager). Any copy of the Inner Layer encryption key should be wiped first before a Crypto Erase is done on the Outer Layer. For example, in a CSfC compliant system using a SED with the KLC Group CipherDriveOne software for the Outer Layer and CipherDriveOne Kryptr as the Inner Layer, a proper CE involves: 1) using Kryptr Erase Disk function to destroy the Inner Layer encryption keys followed by 2) using the CipherDriveOne Erase Disk function to reset the SED to erase Outer Layer data. It should be noted that - in this case - the Erase Disk functionality requires an Administrator or Security Officer role and cannot be done by a regular User.

[3] COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC) Data-at-Rest Capability Package V5.0 – Nov. 2020
[4] See requirement DAR-EU-21 in the CSfC Data-at-Rest Capability Package V5.0.