Seagate Secure™ Certified Erase Protects Data and Enables The Circular Economy

Statistics show that about 600 Million new Hard Disk Drives (HDD) and Solid State Drives (SSD) are sold and put into service each year. Seagate sold a whopping 367 Exabytes of data in calendar year 2018. This is more than an exabyte per day! And according to the IDC Data Age report, the global datasphere is only going to continue to grow—from 33 Zettabytes in 2018 to over 175 Zettabytes in 2025.

This data storage growth means an increasing amount of data and storage devices are taken out of service, repurposed, reused, recycled, and/or enter landfills. The data on these drives is subject to pervasive global data privacy laws, such as the EU General Data Protection Regulation (GDPR) and the U.S. Health Information Portability and Accountability Act (HIPAA), intellectual property regulations, and data breach regulations—all with severe financial and brand penalties for data breaches.

Global regulations increasingly favor reused and recycled content in all products, and overall environmental considerations dictate a more circular economy approach. This trend favors reuse and recovery of components over raw-material recycling and landfills for used HDDs and SSDs.

Although the environmental and economic benefits of reuse and recycling of storage devices are evident, there is a risk of unintended data disclosure. Organizations and individuals might hesitate to return devices for reuse unless data stored on drives was properly purged. With standardized and certified data erasure capabilities we can avoid negative data loss consequences and move toward a more environmentally responsible life cycle for all of these drives.

Media Sanitization Standards

Seagate has led and partnered with the Industry, standards bodies, and regulatory authorities to achieve unified standards for media sanitization.

Upon publication in December of 2014, the National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1 became the unified US federal media sanitization guideline while deprecating a multitude of other standards (e.g., DoD 5220.20M). NIST SP 800-88 R1 defines the data risk management framework for disposition of many media types, including HDDs and SSDs, while providing three levels of erasure as follows:

- "**Clear**: applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge**: applies physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques.
- **Destroy**: renders data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data."

NIST SP 800-88 R1 goes on to sanction multiple forms of data Purge, including standardized and drive atomic data overwrite, block erase, and cryptographic erase commands. These commands are standardized in accordance with the Trusted Computing Group Storage Specification, ANSI T10 (SCSI), ANSI T13 (ATA), and NVM Express command interface standards. It defines the NIST standards for cryptographic best practices and the information collected about the erasure event that can be used for certified erase services. Additionally, the NIST SP 800-88 R1 provides guidance for physical destruction in case the device has become inoperable.

In addition to the NIST standard, the International Organization for Standardization (ISO) published the ISO/IEC 27040:2015 standard. This standard has also adopted these Media Sanitization norms, representing the common and unified international standard for erasing the data on HDDs, SSDs, and other media types.

With the ISO and NIST standards, we have a unified federal and international baseline for HDD and SSD erasure, and certificate of erasure.

Seagate Secure Enables Certified Erase

Seagate HDDs and SSDs with the Seagate Secure logo provide essential and certified security for strong data-at-rest protection and high assurance of certified erasure of data.

The Seagate Secure essential feature set provides cryptographic device and firmware protections along with secure supply chain compliance according to the ISO 20243 Standard, providing assurance of the integrity and authenticity of the drives.

Seagate Secure certified devices undergo rigorous security validation according to the Cryptographic Module Validation Program (CMVP) and the NIST FIPS 140-2 standard. This validation ensures that the security services and cryptographic requirements of NIST 800-88 R1 are met and validated by an independent lab.

The Seagate validation certificates can be found online at the NIST CMVP website.

Seagate Secure certified devices lead the industry with Common Criteria validation to the FDE Encryption Engine collaborative Protection Profile. A successful Common Criteria evaluation is required to obtain security certification by the Trusted Computing Group. Additionally, successful Common Criteria evaluation is required to qualify devices for use in classified data environments in up to 28 member nations recognizing this certification. Common Criteria validation requires successfully passing an independent lab evaluation of the Self Encrypting Drive security model, including validation of the erase functions, validation of proper keychain design, validation of key wrapping design, and validation of key destruction on cryptographic erase. The Seagate validation certificates can also be found online at the Common Criteria website.

Seagate Certified Erase Solution

With Seagate Secure certified drives across our portfolio, Seagate is uniquely positioned to provide the highest levels of assurance for certified erasure services. The certificate of data erasure is digitally signed by the private keys of the drive and meets the NIST 800-88 R1 Erasure Certificate requirements.

The solution provides the Common Criteria and FIPS 140-2 levels of assurance for drive erase functionality, security, and cryptography along with an immutable certificate of erasure which can be verified to be authentic to each drive and Seagate.

With Seagate Secure Certified Erase, you get the strongest assurance of compliance for data protection. Seagate is currently piloting certified erase internally and initiating pilots with our customers. We look forward to the global ubiquity of certified erase services for data protection, an effort that will help enable a circular economy.

Monty A. Forehand, Product Security Officer
Manuel A. Offenberg, Security Technologist, Seagate Research Group
5 November 2018 (updated 20 May 2019)

Footnote: *1 Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, Dec 2014, Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine

seagate.com