Technology Paper

# Trusted Life Cycle for Product Authenticity

March 1, 2019

## Contents

# Ensuring a Trusted Life Cycle

## Executive Summary

Seagate understands the most valuable asset in any storage system is the data itself. Seagate was an early adopter and leader in the development of drive-level encryption technologies and recognizes this is only a small part of any true security strategy. Today customers are beginning to recognize the importance of integrating authentic system components that have been validated from the manufacturer by establishing Secure Supply Chain requirements. Through the efforts of the recently developed Product Security Office (PSO), Seagate has adopted the Open Trusted Technology Provider Standard (O-TTPS) to span technology development from the supply chain through the delivery of products to our customers. Seagate upholds an industry-leading firmware attestation process to ensure customers receive authentic products, components, and firmware. Due to the negative publicity and increased penalties stemming from breaches and errors in data management and retirement policies, data storage and protection is truly a product life cycle consideration that must be thought of with a "layered" or redundant approach. This white paper explores how Seagate ensures a trusted life cycle for manufacturing and firmware development process, by using features such as Secure Download & Diagnostics (SD&D), Secure Boot, and Instant Secure Erase (ISE).

## Design, Component Purchase, and Manufacturing

Seagate has established the PSO to ensure supply chain compliance to a standards-based set of security policies known as the Open Trusted Technology Provider ™ Standard (O-TTPS). O-TTPS consists of two main components with the intention of ensuring "integrity in technology deployment and to prevent maliciously tainted and counterfeit products from entering the supply chain" (https://ottps-cert.opengroup. org). In Seagate's context, the ultimate objective is to ensure a critical group of component suppliers comply with O-TTPS requirements so that storage products are authentic and minimize supply chain cybersecurity risks. A multi-phased approach to O-TTPS supplier compliance is underway by Seagate, and the most critical electrical component suppliers are now in the self-assessment phase (Phase 2) of the process. Seagate's plan is to document compliance from all critical suppliers.

In addition to O-TTPS compliance, Seagate has an extensive supplier qualification process to ensure component manufacturers deliver products compliant with original Seagate designs. Final confirmation of component and drive authenticity takes place during the Seagate drive test process as firmware is introduced to the end hard disc drive (HDD).

## Firmware Control Threats

Beyond hardware design and manufacturing, hard disc drive (HDD) firmware – which is impossible for upper stack antivirus programs to scan – is often overlooked. The firmware of an HDD has the difficult task of managing and preventing loss of the most vital asset – customer data – and Seagate has focused on this design element to prevent rogue firmware and malware that has the potential to pose significant threats when used to execute malicious software in IT environments. Seagate has evaluated potential firmware threats to its products and identified the following crucial elements of firmware design and implementation:

1. Developing and validating an authentic code.
2. Securely delivering the code to the hard disc drive manufacturing sites.
3. Ensuring authentic code was loaded onto the drive, tested, and the drive is malware free.
4. Validating no tampering occurred with the drive during shipment.
5. Validating an authentic product, including hardware, firmware, and no malware, upon customer receipt.
6. Continual authentication of firmware during deployment and operation.
7. Quickly sanitizing drives before they are retired to protect customer data while optimizing operational throughput.

# Ensuring a Trusted Life Cycle

Seagate has developed a solution known as Secure Download & Diagnostics (SD&D) that offers critical counterfeit protection, ensures field and factory firmware security and integrity, and ships as a standard feature on every Seagate HDD. SD&D prevents unauthorized access to a drive's firmware and blocks tampering with firmware executables and sensitive system-level data. We will explore each of the above seven vulnerabilities in more detail to highlight how Seagate SD&D and other value-added security features protect our customer's firmware supply chain.

### 1. Developing and Validating an Authentic Code

Every firmware code is subjected to rigorous review and testing during development in compliance with Seagate's security standards. Code reviews are mandatory for all code check-ins, and the security code is restricted by role-based access control. Additionally, all code changes must pass static analysis testing prior to being added into code lines. Beginning here, all Seagate products and configurations are built on a strong security foundation that periodically goes through meticulous on-site testing (black box and white box) by independent labs accredited by the National Institute of Standards and Technology (NIST). This testing validates Seagate's implementation of the latest NIST approved security algorithms, the backbone to a unique process designed to mitigate cyber threats.

### 2. Securely Delivering the Code to the Manufacturing Site

Following development of the firmware at Seagate's design centers, final codes are documented on engineering change requests (ECRs) and placed on the final bill of material (BOM) for each product. Seagate uses a digital signature process compliant with RSA 2048 to protect the authenticity and integrity of the code. The digital signature process utilizes cryptographically strong public-private key hashing algorithms in accordance with Secure Hash Algorithm (SHA) 256 to ensure the code identified on the BOM is received in the factory for flashing to the drive during manufacturing. In this manner, Seagate ensures that code designed for a specific drive and customer in Seagate's design centers is the only authentic code that can be loaded onto the drive during the manufacturing and testing process.

### 3. Ensuring Authentic Code was Loaded and Tested during Manufacturing

Once HDDs are assembled, the next step involves loading firmware to make the drives functional. The firmware load process includes two key steps; configuration verification and rogue firmware detection. Through a customer configuration verification process (ccverify), Seagate ensures only the customer's data pattern is written onto the disc platter. Also, Seagate has developed a new firmware verification protocol known as Rogue Firmware Detection (RFWD). This monitoring process checks the validity of the firmware signature at multiple stages throughout drive production, ensuring that the finished product firmware matches the exact firmware signature intended. The process is monitored 24×7 by a designated team of engineers who can immediately respond to any incident with appropriate security measures.

During this stage in the manufacturing process, the drive BOM is verified to ensure it contains authentic components and all drives are assigned unique keys as part of an automated authentication protocol and can be combined with other technology. The assignment of unique keys during this step allows other security and authentication technologies to be used throughout the product life cycle. Upon leaving Seagate manufacturing facilities, it is in this manner that drives are confirmed to contain authentic components, authentic firmware, and are malware free in the customer's configuration.

### 4. Validating No Tampering Occurred with the Drive During Shipment

The HDD supply chain for a customer begins at one of the Seagate's Global HDD manufacturing sites. Drives are shipped via a combination of commercial truck, ocean freight, and airplanes to the customer's integration site. During shipment, control of the product resides with the commercial carrier of record and crosses many borders worldwide. Additionally, there could be instances when original equipment manufacturer (OEM) customers buy drives from the global distribution network on the open market to service urgent supply chain requirements. Commercial transit and multi-level supply chains require the assurance of authenticity and prevention of tampering or malware on IT products from this process.

Seagate understands this risk and through its SD&D assurance process, all drives shipped from Seagate factories have a locked diagnostics port. This feature blocks unauthorized users from downloading firmware or accessing the drive's installed firmware by requiring user authentication via a Seagate Secure Server to unlock the port. With this added layer of protection on all Seagate drives, tampering with firmware executables and system-level data is prevented. In addition to locking the diagnostics port, SD&D employs forensic logging to trace unauthorized attempts to load or manipulate firmware. Through this combination of protective services, Seagate HDDs offer positive firmware attestation capabilities during the shipping process.

Seagate also provides value-added capabilities to protect against physical tampering and to comply with US government purchasing requirements. For customers who require the ability to detect physical tampering with a drive or its components, tamper evident labels (TEL) on the top cover and printed circuit board assembly (PCBA) are available. This is a concern of many government-grade products, and Seagate was the first HDD manufacturer to develop a TEL solution to comply with NIST Federal Information Protection Standard (FIPS) 140 Level 2. Seagate has also developed capabilities to flash firmware closer to our customer use points in the United States and other compliant countries which enables the drives to meet government contract purchasing requirements set forth in the Trade Agreements Act (TAA).

### 5. Validating an Authentic Product and Code are Received by the Customer

In addition to drive firmware security, an added consideration is how to mitigate threats posed by rogue drive access with malware installation on the drive itself during transport from Seagate's manufacturing site to the customer's deployment site. It is obvious that unless products are physically locked in a safe, transport via truck, ocean freight, and airlines present obvious security risks. Using Seagate's SD&D and ISE capabilities, customers can address these risks as part of a robust deployment process. One option is to utilize Instant Secure Erase (ISE) capable drives to cryptographically erase the contents of the drives upon receipt at the customer's site to ensure no tampering of data on the drive occurred during transport. This technique is commonly used today to ensure drives are deployed without malware or viruses. Additionally, customers can work with Seagate to "lock" the Firmware Download port on drives as part of the manufacturing process and subsequently "unlock" it with a unique drive key. This lock/unlock option of the Firmware Download port, along with the locking of the diagnostics port, would prevent the loading of malware or viruses on the drive's firmware via unauthorized access while being transported.

An added layer of security designed in Seagate's SD&D feature set is Cryptographic firmware signing. Through a formalized and secure Public Key Infrastructure (PKI) deployment process at the receiving site, customers can add a step in the receipt process to ensure encrypted signatures in firmware are required from the host to launch (via Secure Boot) and to enable firmware downloads (via Locked Diagnostics Port and Firmware Authenticity and Integrity Verification). This capability is unprecedented in the HDD industry as Seagate has developed a uniquely hardened and scalable process to support all drives in its product portfolio.

### 6. Ensuring Authentic Code is Used During Customer Deployment

During deployment at a customer's site, Seagate's SD&D feature set continues to provide added layers of run-time authentication. Secure boot is another standard measure with SD&D that prevents a host OS from loading if the firmware's encrypted signature has been changed in any way; firmware signature is authenticated by the drive at host startup. Secure boot is "always on" throughout a drive's life cycle and handshakes with firmware authenticity and integrity verification, another element of the SD&D feature set. Upon start-up, the HDD checks for an encrypted signature in the firmware that attempts to download; firmware is rejected if it is not authenticated as an original Seagate firmware download. This takes advantage of the cryptographic firmware signing feature in SD&D, such that if malicious code is executed inside an authentic copy of an HDD's firmware, SD&D's tamper-evident binary feature enables any altered code to be identified and the firmware blocked from download. This is especially important as a preventative measure during run-time at a customer's site.

### 7. Quickly Sanitizing Drives before Retirement

Beyond a drive's useful life cycle, Seagate also offers additional capabilities to enable customers to provide added security measures in drive retirement processes. ISE, a fast and complete data disposal methodology, allows customers to quickly erase drive data prior to device retirement or as an added measure along with physical destruction policies. Seagate's implementation of ISE meets strict US Government NIST 800-88 compliance standards.

ISE drives, unlike SED drives, do not protect data at rest; but once the encryption key is deleted, no data on the disk can be recovered. This quick-erase functionality can remain dormant unless "unfrozen" at boot via a secure mechanism to ensure that data is not lost by accident or by malicious intent.

## Conclusion and Relevance to Advanced Security and Data Protection

The worldwide IT supply chain continues to face increasing threats from malicious attacks. Security has risen to the forefront as users place more trust in their secure provider to protect their critical data and personally identifiable information. Seagate understands the HDD's role as the last line of defense closest to, managing, and storing customer's data. Through its creation of the Product Security Office (PSO), supply chain compliance to O-TTPS standards, and inclusion of SD&D capabilities with chain of trust features like Secure Boot – all at no additional cost to the customer – Seagate raises the bar in protection of key assets on its HDDs and is the demonstrated industry leader in storage device security. Beyond these base capabilities, Seagate also offers value-added security functionality in physical tamper evidence with FIPS 140 Level 2 NIST certified drives, and the only vendor to have Common Criteria certified, along with Self-Encrypted Drives (SEDs), and ISE  Seagate considers this technology a baseline "required to play" consideration and continues to push forward with new PSO initiatives, as well as future-evolving requirements such as Common Criteria certification and TAA compliant HDDs and solid-state drives (SSDs).

This white paper is intended to help raise awareness to Seagate's approach to cybersecurity as it relates to ensuring authentic devices and a trusted life cycle.

## References


- NIST Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- NIST Special Publication 800-88 Guidelines for Media Sanitization: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf
- Open Trusted Technology Provider ™ Standard (O-TTPS), Version 1.1.1: https://publications.opengroup.org/c185-1
- Maximize Security, Lock Down Hard Drive Firmware with Seagate Secure® Download & Diagnostics Technology Paper: https://www.seagate.com/files/www-content/solutions-content/security-and-encryption/en-us/docs/seagate-secure-download-diagnostics-with-maximize-sec-lock-down-hard-drive-firmware-tp684-1-1508us.pdf
- Public Key Infrastructure (PKI): https://en.wikipedia.org/wiki/Public_key_infrastructure
- NIST Certificates for Seagate's Strong Security Foundation: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm
- Crypto Module Validation Program (CAVP) by NIST with Algorithm Validation Lists: http://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

# Ensuring a Trusted Life Cycle

## Glossary of Terms

- AES 256 Encryption: AES 256 is the advanced encryption standard approved in 2001 by NIST for the encryption of electronic data. AES is available in many key sizes, and 256 identifies that 256-bit keys are used for encryption. 256 is currently the largest bit key size for AES encryption. AES 256 encryption is used by Seagate for its current generation of encrypted drives. It was introduced in NIST as U.S. FIPS PUB 197.
- NIST: The National Institute of Standards (NIST) was founded in 1901 and is now part of the US Department of Commerce. NIST plays a large role in establishing standards for data encryption and certifies independent laboratories for security testing. NIST established the Federal Information Processing Standard (FIPS) as a computer security standard used to approve cryptographic modules.
- NIST 800-88: NIST standard for media sanitization and disposal.
- Open Trusted Technology Provider ™ Standard (O-TTPS): O-TTPS is a standard set of guidelines being adopted to protect against maliciously tainted and counterfeit products throughout the supply chain and product life cycle. The objective of O-TTPS is to establish a standard and develop a certification program for supply chain partners to meet product integrity and supply chain security per the standard.
- RSA 2048: Key generation standard recommended by NIST for public key authentication.
- Secure Boot: Secure Boot uses Public Key Infrastructure to ensure that drives are not allowed to boot without an acceptable firmware signature. Advanced Secure Boot implementations also allow for revocation of known bad signatures in cases where a security vulnerability is found in previously signed firmware.
- Common Criteria: Following a rigorous evaluation by independent industry authorities, Seagate® has achieved Common Criteria accreditation for select products in our Nytro®, Exos™, and BarraCuda® portfolios—meaning they meet internationally-recognized regulations across 28 member nations and are certified for classified environments within those countries.
- SHA 256: Secure Hash Algorithm (SHA) is a method for assigning signatures to a text or data file. The number 256 indicates the use of a 256-bit (32-byte) hash, or one-way function. SHA 256 is used by Seagate to ensure design code signatures match manufacturing code signatures for the transport and use of authentic firmware. SHA 256 was introduced in FIPS PUB 180-2, NIS

**seagate.com**

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00