

# Seagate's self-encrypting laptop hard drive wins key government certification

September 14 2010

---

Seagate today announced that its groundbreaking Momentus Self-Encrypting Drive, the world's first laptop hard drive with built-in encryption to protect against unauthorized access to information on lost or stolen mobile computers, has secured FIPS 140-2 certification from the U.S. National Institute of Standards and Technology (NIST).

The key government certification clears the way for deployments of Momentus Self-Encrypting Drives (SEDs) by all U.S. and Canadian federal agencies, many state and local governments, and regulated industries such as healthcare, finance and defense required to use FIPS-certified gear to help protect [sensitive data](#) on PCs and computer networks. Many utility, education and transportation entities also have adopted the FIPS (Federal Information Processing Standard) 140-2 standard to lock down confidential information. Foreign governments in addition to Canada also recognize FIPS-validated products. The Momentus SED is the first [hard drive](#) with native [encryption](#) to earn the FIPS certification.

“The FIPS 140-2 certification exemplifies Seagate’s commitment to security standards that enable the widespread adoption of encrypting hard drives for laptops and other computers as the explosive growth of laptop PCs puts more sensitive personal and business information at risk,” said Dave Mosley, executive vice president of Sales, Marketing and Product Line Management at Seagate. “Today’s NIST approval gives our system builder and end-user customers the peace of mind that Momentus Self-Encrypting Drives deliver the full power of government-

grade security.”

The FIPS 140-2 seal of approval comes three years after NIST, the federal agency focused on promoting product innovation by establishing technical standards for government and business, certified the Advanced

Encryption Standard (AES) chip built into the Momentus drive. Seagate has shipped more than a million of its self-encrypting laptop drives since their introduction in 2006.

Momentum SEDs give organizations of all sizes a simple, cost-effective way to protect against unauthorized access to data on notebook PCs and a powerful tool for complying with the growing number of data privacy laws calling for the protection of consumer information using government-grade encryption. The AES encryption chip in the Momentum SEDs automatically and transparently encrypts all drive data, not just selected files or partitions. The 2.5-inch drive also eliminates disk initialization and configuration required by encryption software, allows IT administrators to instantly erase all data cryptographically so the drive can be quickly and easily redeployed, and delivers full inline-speed encryption with no impact to system performance.

Momentum SEDs keep all security keys and cryptographic operations within the drive, separating them from the operating system to provide greater protection against hacking and tampering than traditional software alternatives, which can give thieves backdoor access to encryption keys and are otherwise more vulnerable to key theft. With third-party management software, organizations can easily and affordably manage and protect encryption keys and passwords. Momentum SEDs are offered in capacities up to 500GB.

**More information:** See Seagate’s FIPS 140-2 certificate here: [csrc.nist.gov/groups/STM/cmvp/ ... 40crt/140crt1388.pdf](https://csrc.nist.gov/groups/STM/cmvp/.../40crt/140crt1388.pdf) .

Source: Seagate

Citation: Seagate's self-encrypting laptop hard drive wins key government certification (2010, September 14) retrieved 26 April 2024 from <https://phys.org/news/2010-09-seagate-self-encrypting-laptop-hard-key.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.