

SPYRUS has a long history of providing high-assurance security technology for the U.S. Government, and we have some of the best technologists in the world working for us. This version of the press release that SPYRUS recently distributed provides additional technical details for those who are interested. We hope that you find it informative.

## **Kingston Digital Launches New DataTraveler 5000 with Secured by SPYRUS™ Patented Technology**

SPYRUS High-Assurance Elliptic Curve Cryptography Hardware Designs Create the Most Advanced Secure USB Product Offerings Available

**San Jose, California, January 28, 2010** – SPYRUS, Inc., today announced that their Secured by SPYRUS™ technology is used to implement all cryptographic security functions in the new Kingston DataTraveler® 5000 USB flash drive. The DataTraveler 5000 will be available to government and enterprise customers in over 100 countries.

In 2009, SPYRUS and Kingston partnered to leverage Kingston's worldwide leadership position in manufacturing memory products and over 15 years of SPYRUS experience pioneering hardware-based security technologies. The Secured by SPYRUS™ elliptic curve cryptography and encryption technologies used in the DataTraveler 5000 were originally designed to protect sensitive government data. The DataTraveler 5000 is the most advanced USB encryption drive designed to protect your secrets.

“SPYRUS designed its hardware-based security to protect U.S. Department of Defense and other sensitive data. We are proud to join with Kingston to introduce a product with many of the same high-assurance technologies used in our own Hydra PC™ product line,” said Tom Dickens, Chief Operating Officer for SPYRUS. “Our proven technologies surpass all others to protect customer data against the proliferation of cyber crime, cyber attacks, and data loss.”

The DataTraveler 5000 employs the SPYRUS Suite B On Board™ hardware implementation of the advanced Elliptic Curve Cryptography (ECC) P-384 and AES-256 algorithms. These same algorithms are used by the U.S. Government to protect both unclassified and classified data at the TOP SECRET level, in approved implementations.

The DataTraveler 5000's FIPS 140-2 Level 3-compliant epoxy-sealed cryptographic boundary (formal Level 3 certification is pending) includes the entire flash memory, along with multiple security processors that cooperate to implement and verify the accuracy of the various cryptographic functions. This Secured by SPYRUS™ hardware module uses patented SPYRUS technologies to add further protection to key management and key encryption operations and shield the cryptographic processing from electronic eavesdropping.

When the DataTraveler 5000 is inserted into a computer, an EC Diffie-Hellman key agreement is used to establish an AES-256-encrypted secure channel, which securely transfers the user's password from the computer to the security processor within the cryptographic boundary of the device. No keys or other critical security parameters are ever exposed outside the cryptographic boundary.

Within the secure cryptographic boundary, the user's password is combined with high-entropy sources using FIPS-approved key derivation techniques to unlock a secure key hierarchy that protects the encrypted contents of the drive. The initial password and the derived key are never stored in nonvolatile memory, either on the host computer or on the DataTraveler 5000, not even in hashed form. No authorization codes travel between the device and the host computer; and keys are never present on the host computer, where they could be compromised.

If the right password is entered, the drive is unlocked and decrypted; otherwise, the password is rejected and the count of incorrect password entry attempts is incremented in the hardware. If the maximum number of attempts is exceeded, further use of the device is blocked until it is reinitialized by a system administrator. As a result, the DataTraveler 5000 is completely immune to password-guessing, offline exhaustive search attacks. Vulnerabilities that have plagued many other USB encryption drives have been eliminated in this new design.

Although many other devices use AES-256 encryption, the DataTraveler 5000 is the first hardware-based, FIPS 140-2-validated encryption product in the industry that uses the newly standardized XTS-AES mode of sector-by-sector media encryption. XTS-AES uses a form of double-encryption and is significantly stronger than the conventional ECB or CBC modes of operation used by other devices. The Secured By SPYRUS™ technology is unique in the industry in its use of the exceptionally strong Suite B ECC P-384 algorithms and keys (the equivalent of a 7,680-bit RSA key) to protect the AES-256 key. Other products use RSA-2048 (equivalent to only 112 bits of cryptographic strength) or password-based encryption to protect the keys, which may provide as little as 26 bits of overall strength.

The DataTraveler 5000 Secured by SPYRUS™ delivers unsurpassed levels of security and encryption to government and enterprise customers. This portable data solution represents state-of-the-art data protection with the simplicity of plug and play. The drive is optionally available with SPYRUS Sentry A-V software to ensure the security of the host computer.

Secured by SPYRUS™ confirms that the device implements cryptographic technologies and processor modules that have been developed and proven by SPYRUS in over 15 years of leadership in the commercial development of the most secure hardware-based encryption, authentication, and digital content security products available to governments, enterprises, and military organizations.

### **About SPYRUS, Inc.**

SPYRUS holds patents in the U.S. and abroad that enable solutions for secure authentication, secure communication, and full disk encryption, as well as patents relating to data protection and rights management for digital content. Secured by SPYRUS™ security technology is designed, developed, and manufactured in the USA to meet FIPS 140-2 standards. SPYRUS products support the strongest commercially available cryptographic algorithms, including elliptic curve cryptography (ECC), AES, and SHA-2, collectively known as Suite B. In December 2007, the Hydra PC Personal Encryption Device became the first, and as yet the only, commercially available USB encryption device to be approved for protecting U.S. Government tactical classified data at the Secret level and below, when used in accordance with the approved operational security doctrine. SPYRUS is headquartered in San Jose, California. See [www.spyrus.com](http://www.spyrus.com) for more information.

### **About Kingston Digital, Inc.**

Kingston Digital, Inc. (“KDI”) is the Flash memory affiliate of Kingston Technology Company, Inc., the world’s largest independent manufacturer of memory products. Established in 2008, KDI is headquartered in Fountain Valley, California, USA. For more information, please visit [www.kingston.com](http://www.kingston.com) or call 800-337-8410.

SPYRUS, the SPYRUS logo, Hydra Privacy Card and Hydra PC are either registered trademarks or trademarks of SPYRUS, Inc., in the U.S. and/or other jurisdictions. All other company, organization and product names are trademarks of their respective organizations.

Kingston and the Kingston logo are registered trademarks of Kingston Technology Corporation. All rights reserved. All other marks may be the property of their respective titleholders.

**Editor’s Note:** For additional information or executive interviews, please contact Dan Chmielewski of Madison Alexander PR, Inc. +1 (949-231-2965) or [dchm@madisonalexanderpr.com](mailto:dchm@madisonalexanderpr.com).