
DataTraveler 5000 (DT5000)

Technical Highpoints



Contents


DT5000 TECHNOLOGY OVERVIEW	3
WHY DT5000 ENCRYPTION IS DIFFERENT	2
WHY DT5000 ENCRYPTION IS DIFFERENT – SUMMARY	5
XTS-AES SECTOR-BASED ENCRYPTION	3
SPYRUS BACKGROUND	5

The Licensed Product may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 6,088,802; 6,981,149; 5,761,305; 5,889,865; 5,896,455, 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483; U.S. Pat. Appl. Ser. Nos. 60/886,087; 11/258,596; 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9; PCT/US08/51729.

DT5000 Technology Overview

The DT5000 is the flagship of the Kingston® DataTraveler® Flash drive product line and the culmination of five years of research and development of encryption by SPYRUS, Inc., using what are now called the Suite B algorithms, and in particular the highly efficient Elliptic Curve Cryptography algorithms. These high-strength but unclassified algorithms were specifically selected and approved by the U.S. Government and DoD for use in multi-national data sharing environments, including both classified and unclassified applications. Suite B provides significantly greater strength and much better performance than the RSA algorithms used by other sector-based encryption USB devices. The ECC P-384 keys used within the DT5000 are the equivalent of a 7,680-bit RSA key, yet the ECC operations are faster than RSA-2048, and 64 times faster than an RSA-7680 key would be.

SPYRUS's development of the technology used by the DT5000 was guided by specific design criteria derived from its many years of individual and corporate experience in cryptography in general, and low-cost, high-assurance cryptographic hardware devices in particular. The design criteria used within the DT5000 include the following:

- Dedicated security processor chips for all static key generation and storage, and for user authentication. Designed for the high-assurance, high-volume commercial banking, and defense applications markets, where valuable content must be protected against the threats from millions of public or private users, these devices have numerous DoD applications for embedded security, and they have been extensively analyzed by several national governments and independent national laboratories.
- 
- The SPYRUS logo, which consists of a dark brown square with a white mountain-like shape at the top and the word 'SPYRUS' in white capital letters below it, all set against a light blue background.
- Supplemental dedicated security processors with general-purpose processor chips (e.g., an ARM processor) for higher bandwidth applications, high-speed public key operations, and general control functions, including power-on self-tests and on-going health checks.
 - Implement high-speed symmetric encryption and hash functions in an FPGA (field programmable gateway) for performance and flexibility.
 - Incorporates “approved” high entropy deterministic random bit generators.
 - Prohibit all external key generation and key loading, as well as all private key extraction (key escrow). Too many compromises have occurred as a result of the human element involved in such processes.
 - Uses high-strength Elliptic Curve Cryptography for all key management.
 - Ensure that the key strength of data confidentiality and data integrity mechanisms is sufficient to resist all known attacks for at least 100+ years, or beyond a human lifespan.
 - Designed to meet FIPS 140-2 Level 2 and Level 3 or even more stringent demands, including exotic hacking tools such as electron microscopes, sophisticated chip-peeling techniques, and side channel and timing attacks.

Why DT5000 Encryption Is Different

The DT5000 includes the following SPYRUS™ developed features, which are unique among all competing sector-based media encrypting Flash drives:

- The DT5000 sector-based USB encryption device implements Suite B high-strength cryptographic algorithms and advanced key management, in accordance with Cryptographic Modernization directives, including Elliptic Curve Cryptography (ECC) with P-384 keys, AES-256 and SHA-384. The DoD established the Suite B algorithms as a national standard for national security information. Suite B provides significantly greater strength than the RSA algorithms used by other USB devices.
- If an incorrect PIN is entered and the maximum number of attempts is exceeded, the keys are zeroized and no data stored on the drive can ever be decrypted in the future.

The DT5000 also benefits customers by providing security for encryption key management that is more extensive than FIPS 140-2 standards, namely:

- The strength of AES-256 encryption keys is not defined by the encryption algorithm *per se*, but by the entropy or randomness of the bits composing the keys and by the strength of the public key algorithms used to communicate and protect those bits. DT5000 uses approved high-assurance random number generation techniques to create high-entropy keys in accordance with NIST SP 800-90.
- The continuing strength of the encryption and signatures keys is dependent on the algorithmic and hardware mechanisms used for protecting the keys. All encryption is performed in hardware within a tamper-evident security boundary. Private keys cannot be imported, exported, or corrupted. For added security against “brute-force” attacks, the DT5000 permanently deletes the encryption keys after 10 incorrect PIN entries, rendering the encrypted data undecipherable.
- DT5000 does not store the PIN internally, even in a hashed form. Instead, the user’s PIN is entered over a secure channel and is mathematically combined with other information using Suite B algorithms to generate a Master Key Encryption Key which is then used to protect the Media Encryption Key.
- DT5000 supports digitally signed firmware using ECDSA P-384 and SHA-384 cryptography.
 - Signed firmware updates are a new security requirement established by the U.S. DoD for encrypting USB flash drives.

XTS-AES Sector-Based Encryption

The Kingston DT5000 uses the more robust strength of XTS-AES sector-based hardware media encryption, to address certain vulnerabilities of conventional encryption modes, such as Electronic Code Book (ECB) to known attacks which make such schemes questionable for disk and media encryption.

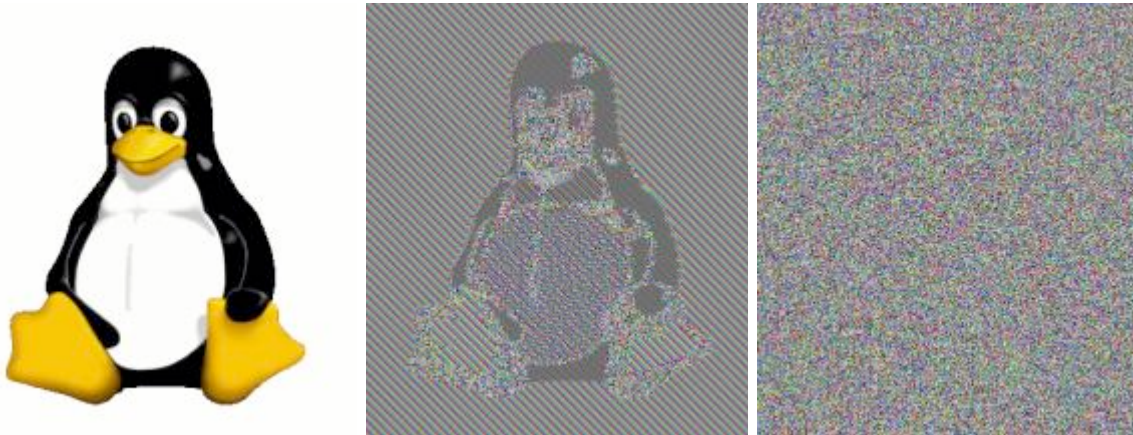
NIST recently addressed this issue in SP800-38E. This standard endorses the IEEE P1619 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, with a new Mode of Operation called XTS-AES, which is particularly well-suited for sector-base media encryption and far superior to competing implementations.

- ✚ NIST SP800-38E is a new security standard referenced by the U.S. DoD for encrypting USB flash drives.

The problem that XTS-AES addresses (and that other modes do not) is that with media encryption and fixed-length sectors, there is no room to store the random Initialization Vector (IV) that normally is used to protect against replay attacks. As a result, a substitute must be used

for an IV, based on the logical sector number. However, because that field is predictable, various attacks become feasible, including so-called watermarking and replay attacks.

Alternatives used by competing products, such as Electronic Code Book (ECB) mode, have serious weaknesses. For example, because a single key is used to encrypt the entire disk or media, encrypting a known (or guessed) block of plaintext in ECB mode will generate a specific block of output in every case, no matter where on this disk it happens to occur. This significantly eases the work of the attacker, as pieces of a message may make use of fragments that are known in other contexts.



Original

Encrypted using ECB mode

Encrypted using other modes

As the above pictures (from http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation) make clear, ECB mode is far from ideal, because the same plaintext always generates the same ciphertext — there is no mixing or diffusion of information that would make the encryption vary according to the context or the location on the media. Not only can this leak information across files written at different times, it can also leak information within a file, for example if a word or phrase is repeated.

Other Modes of Operation are even worse, when used for sector-based media encryption. Output Feedback Mode (OFB), Counter Mode (CTR), and Counter with CBC-MAC (CCN) all operate similarly. They all generate a string of pseudo-random bits that begins with some starting point (an Initialization Vector), and that string is then exclusive-ORed (XORed) with the plaintext that is to be encrypted. However, the Initialization Vector is derived from the sector number and therefore never changes, and thus the string of random bits used to encrypt a particular sector is always the same. Now consider what would happen if it were possible for an attacker to copy all of the encrypted sectors on the device at some initial point in time, and then copy all of the encrypted data again at some later time. Assuming some of the data has changed, it would be possible to exclusive-OR the two versions of the changed sector together. This would have the effect of cancelling out ALL of the random encryption bits, and leave the XOR of the two plaintext strings as a result. Because of the redundancy in any natural language, it is a trivial matter to decode such a result.

The XTS-AES block encryption algorithm solves these problems through what is called a “tweakable” cipher¹ that adds additional security. With this scheme, TWO full-strength AES-keys are used. The first is used to generate what is called a *tweak*, which is an encrypted function of the logical sector number plus a continuing polynomial permutation, so that no two sectors on the storage medium are processed in exactly the same way. The permuted tweak is used to “pre-whiten” the plaintext before encrypting it, and later to post-whiten the ciphertext output. This prevents the adversary from decrypting any sector of the disk by copying it to an unused sector of the disk and performing an unauthorized decryption. It also prevents two identical plaintext sectors in different locations from encrypting to identical ciphertexts and thus leaking potentially useful information to an attacker. In effect, XTS-AES is using TWO AES-256 keys to triple-encrypt a sector in a manner reminiscent of two-key triple-DES but with much stronger keys.

The result is that the Kingston DT5000, using the XTS-AES technology developed by SPYRUS, is significantly more robust than any other sector-based media encryption products on the market.

Why DT5000 Encryption Is Different — Summary

The DT5000 includes the following SPYRUS-developed features, which are unique among all competing sector-based media encrypting flash drives:

- The DT5000 is the **only** sector-based USB media encryption device that implements Suite B high-strength cryptographic algorithms, in accordance with Cryptographic Modernization directives, including Elliptic Curve Cryptography (ECC) with P-384 keys, AES-256 and SHA-384. The U.S. DoD established the Suite B algorithms as a national standard for protection national security information and communications. Suite B provides significantly greater strength than the RSA algorithms used by other USB encryption devices.

DT5000 also benefits customers by providing security for encryption key management that is more extensive than FIPS 140-2 standards, namely:

- The strength of AES-256 encryption is not defined by the encryption algorithm *per se*, but by the entropy or randomness of the bits composing the keys and by the strength of the public key algorithms used to communicate and protect those bits. The DT5000 uses high-assurance, random number generation techniques to create high-entropy AES-256 keys, and ECC P-384 keys to protect them. By comparison, products that use RSA-2048 only provide the equivalent of 112 bits of protection for such keys. ***The result is like using a very strong lock on your front door, and then hiding the key under the doormat.***
- The continuing strength of the encryption and signatures keys is dependent on the algorithmic and hardware mechanisms used for protecting the keys. All encryption is performed in hardware within a tamper-evident security boundary. Private keys cannot be imported, exported, or corrupted.
- Uses the XTS-AES encryption mode.
- DT5000 does not store the PIN internally, even in a hashed form. Instead, the user’s PIN is entered over a secure channel and is mathematically combined with other information using

¹ A tweakable block cipher accepts a second input called the tweak along with its usual plaintext or ciphertext input. The tweak, along with the key, selects the permutation computed by the cipher. The XTS-AES tweak cipher was approved as a standard by IEEE P-1619 in December 2007, and endorsed by NIST in SP 800-38E.

Suite B algorithms to generate a Master Key Encryption Key, which is then used to protect the Media Encryption Key.

- A secure channel protects sensitive authentication traffic between the host and the module, using the elliptic curve Suite B cryptography recommended by NSA to protect national security systems and national security information.
- The Kingston DT5000 Security boundary envelopes three separate processors within the cryptographic boundary to conveniently implement cryptographic functions, adding further protection to key management and key encryption operations.
- Finally, if the maximum number of incorrect PIN attempts is exceeded, the keys are zeroized.

SPYRUS Background

SPYRUS provides high-assurance security technology for the U.S. Government, industries required to comply with security regulations, and everyday users who want the best protection for sensitive information. All SPYRUS security technology is designed, developed, and manufactured entirely in the USA. SPYRUS hardware and software support the strongest commercially available cryptographic algorithms, including all Suite B algorithms and legacy algorithms such as RSA and triple-DES.

Kingston Digital, Inc., the Flash memory affiliate of Kingston Technology Company, Inc., the independent world leader in memory products, has partnered with SPYRUS, Inc., the leader in the development and manufacturing of advanced hardware-based encryption, authentication, and digital content security products. Under the collaboration, Kingston will incorporate patented Secured by SPYRUS technology into its DataTraveler USB Flash drives to deliver unsurpassed levels of security and encryption to government agencies and enterprise customers.