www.kingston.com/europe/digitalmedia

# DataTraveler Elite

*Advanced Security and High Performance White Paper*

A leading-edge solution for business and corporate IT users that combines advanced data security with outstanding performance.

Kingston®
TECHNOLOGY

## Introduction

Conveniently small, portable, and easy to use, USB Flash drives have become one of the fastest growing Digital Media products. Many business customers and advanced consumers require key features to enhance their use of USB Flash drives, including advanced security, high performance and file synchronization.

Customers require advanced security to guard against sensitive data loss should the DataTraveler drives get lost, misplaced, or borrowed without permission. They want high-performance drives to speed up data transfers and increase productivity. File synchronization between a computer and the DataTraveler drive allows key data to be backed up and available for use on the road or on other PCs.

Kingston's DataTraveler Elite ("DT Elite") USB Flash drive meets these needs. With the industry's highest performance and two-layer security incorporating hardware-based 128-bit AES encryption, DT Elite is one of the most secure USB Flash drives for Windows®-based systems in the world. In addition, DT Elite incorporates file management and folder synchronization through an easy-to-use TravelerSafe+ file management console. This white paper will provide more details on the advanced security and high-performance features of the DT Elite.

## 1.0 DataTraveler Elite Security Features

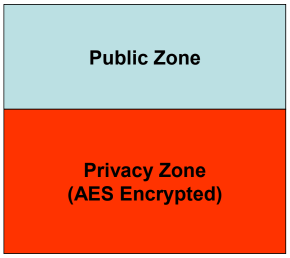
Robust security is the primary feature that was engineered into the DT Elite. A two-layer security mechanism that features user authentication and hardware-based, real-time data encryption guards sensitive data stored on the DT Elite.

DT Elite also has a built-in encryption/decryption co-processor for advanced security and features an industry-leading, high-performance Flash memory controller that offers one of the highest levels of USB 2.0 performance available on the market today.

### 1.1 User Authentication

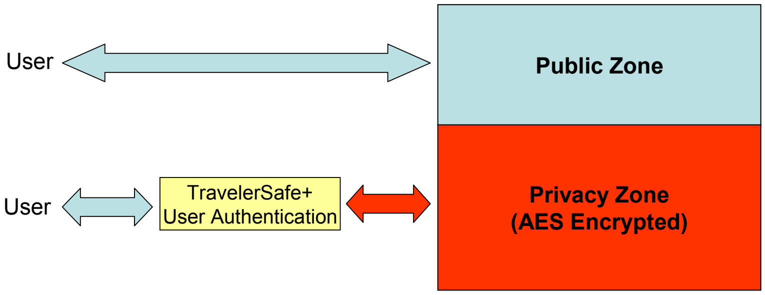
To activate the security features of the DataTraveler Elite, the user must create a privacy zone. As shipped from the factory, the DT Elite drive is set up as a single, public zone. All data stored in the public zone can be read by any host computer.

The owner of the DT Elite creates a privacy zone for the storage of secure data using TravelerSafe+, the DT Elite's access protection software for Windows-based systems. He or she defines a password to control access to the privacy zone, an area on the drive in which all sensitive data is kept. This password is stored in the DT Elite in an encrypted mode that makes it very difficult to decrypt. Once a privacy zone is created using the TravelerSafe+ console, data stored there will be encrypted using the Advanced Encryption Standard (AES-128):



**DT Elite with public and encrypted, password-protected privacy zone (shown in red)**

Without a valid password, unauthorized access to the privacy zone is blocked, and the data remains encrypted and protected. Whenever the DT Elite is connected to a host computer, the TravelerSafe+ console needs to be used to log into and access the privacy zone:



**The privacy zone can only be accessed after valid password logon**

Unlike other software consoles that allow unlimited numbers of incorrect passwords, DT Elite has a factory-set limit that locks the privacy zone after 25 *consecutive* failed attempts to log in. This limit blocks “Brute Force Attacks,” in which programs are used to test millions of password combinations to find the correct password. After 25 consecutive invalid attempts, the DT Elite will lock out the privacy zone; the only option left at this point is to reformat the drive, thus losing all the encrypted data stored in the privacy zone.

### 1.2 Hardware-Based, Real-Time Data Encryption

Cryptography is the science of encrypting and decrypting data using a special “key” to encode and decode the data. Unencrypted data (or files) are processed through an encryption engine (either in software or in hardware) to produce an encrypted file; without the exact key, the data is unusable.

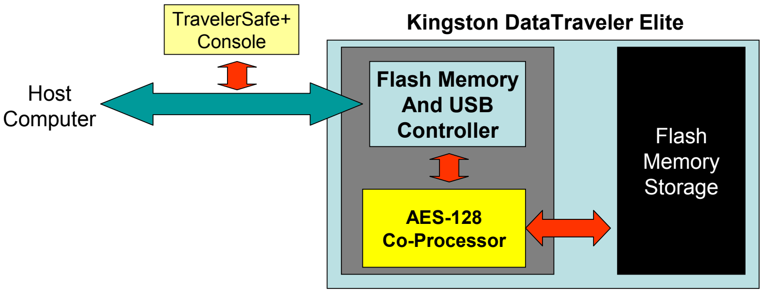
Every DT Elite features one of the industry’s best, most robust data encryption capabilities. The DT Elite’s encryption technology is based upon the same standard used in high-security applications – the Advanced Encryption Standard (AES). Keys are sequences of bits (128 in the case of AES-128) which are used by the encryption/decryption engine to uniquely process the data.

### 1.2.1 Advanced Encryption Standard (AES-128)

The Advanced Encryption Standard was defined by the National Institute of Standards and Technology (NIST) in 1997. Kingston has adopted the AES-128 standard for 128-bit encryption/decryption. With this standard, if a key is used to encrypt data, the exact same key must be used to decrypt the data. Without the same key, data would be a useless string of data.

### 1.2.2 DT Elite's Real-Time, Hardware-Based Encryption

The AES encryption/decryption functions are performed directly in the DT Elite's Flash memory controller.

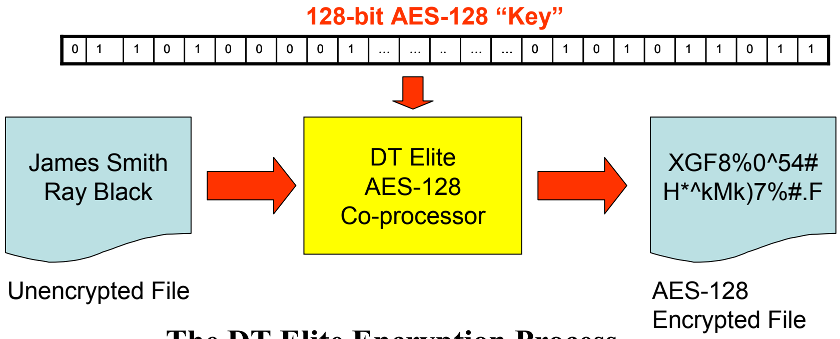


**DT Elite Security Architecture**

When the DT Elite is connected to a host computer, data and file management commands are exchanged between the host computer and the DT Elite Flash memory and USB controller. When data is written to a public zone in DT Elite, the data is written to the Flash memory storage without any encryption. This data can be read on any host computer or other device.

To access the privacy zone, the user is required to use the TravelerSafe+ console and enter a valid password. Once logged in, the host computer will be able to write and read data from the privacy zone.

When data is written to a privacy zone, it is encrypted by the AES Encryption and Decryption Co-Processor in real-time, and then written to the Flash memory storage. Similarly for reads, the data is decrypted real-time on the DT Elite drive and then sent to the host computer.

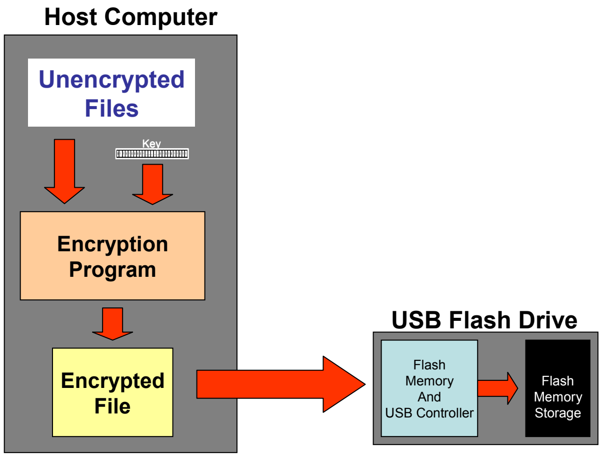


**The DT Elite Encryption Process**

Without the unique 128-bit key, which is uniquely generated for the DT Elite utilizing a true random number generator, encrypted data is nearly impossible to decode.

## 1.3 Software-Based Encryption vs. DT Elite's Hardware-Based AES Encryption

### 1.3.1 Software-Based Encryption



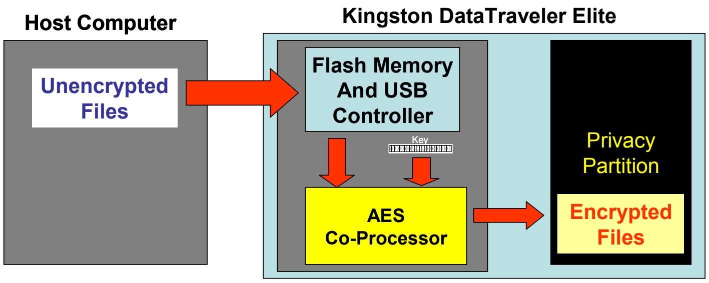
**Software-Based Encryption**

In this case, the user has to explicitly run a program to encrypt a file. When the file is encrypted, the file can then be copied to the USB Flash drive.

When run on host computers, encryption and decryption programs take up a lot of processor resources and reduce overall system performance.

### 1.3.2 DT Elite's Hardware-Based Encryption

Because the processor-intense AES encryption/decryption is done through a DT Elite dedicated co-processor, the DT Elite offers an industry-leading performance level over software encryption programs.



**DT Elite has a Built-in AES-128 Encryption Co-Processor**

In addition, utilizing hardware encryption on the DT Elite itself does not expose the AES “key” to host computers or networks, further increasing security. In the DT Elite, the encrypted user password and the key are never shared outside of the DT Elite. With software-based encryption approaches, the key or keys are exposed to the host computer and network.

As can be seen in the Benchmarking section, there is no performance penalty when storing files on the public and privacy zones in a DT Elite (see **section 3.2.3**).

| | DT Elite<br>with built-in, hardware-based encryption/decryption | Other USB Drives<br>with Software-based Encryption |
|---|---|---|
| Invalid Password Retry limit | Yes | Rare |
| Advanced hashing (encoding) of user password to secure it | Yes | Varies |
| Dedicated AES co-processor on USB drive | Yes | No |
| Data encrypted/decrypted on host computer | No | Yes |
| AES key exposed to host computer or network | No | Yes |
| Performance penalty | No | Yes (40-50% slower) |

**Benefits of DT Elite’s Hardware-Based Encryption vs. Software Approaches**

## 1.4 Additional Certifications

The Kingston DT Elite has the following certifications:

- Hi-Speed USB 2.0
- WHQL for Windows XP, Windows 2000 and Windows ME

The DT Elite also meets the provisions of the Cryptography Note (Note 3) in Category 5, Part 2, of the Commerce Control List (United States Department of Commerce – Bureau of Industry and Security – Encryption regulatory).

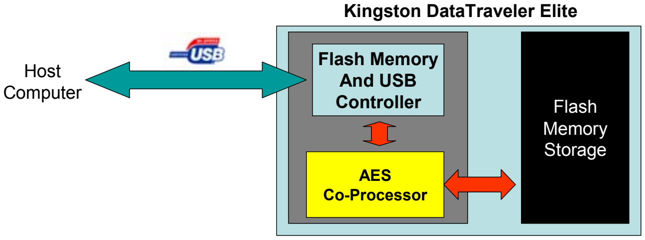
## 2.0 DataTraveler Elite Performance

Kingston’s DT Elite is engineered with a state-of-the-art, Hi-Speed USB 2.0 controller that delivers outstanding performance. Even when AES-128 encryption/decryption security is used, the DT Elite’s performance is not reduced due to its built-in AES-128 co-processor. DT Elite makes no performance compromises while delivering an advanced level of security.

| | Read Data Transfer Rate (Peak) | Write Data Transfer Rate (Peak) | Public/Privacy Zone Support | Advanced Security |
|---|---|---|---|---|
| DataTraveler Elite | 24 MB/sec. | 14 MB/sec. | Yes | Yes<br>(Hardware AES-128) |
| DataTraveler II Plus | 19 MB/sec. | 13 MB/sec. | Yes | No |
| DataTraveler II | 11 MB/sec. | 7 MB/sec. | Yes | No |
| DataTraveler | 6.5 MB/sec | 1.5 MB/sec. | No | No |

**Kingston DataTraveler Transfer Rates and Security Features**

### 3.1 Hi-Speed USB 2.0 Interface



**The DT Elite Features a Certified, Hi-Speed USB Interface**

Because the USB Hi-Speed standard is a range (for more information, please see Kingston's Digital Media Guide at kingston.com/Digital_Media_guide), products can offer different performance levels despite having the same Hi-Speed USB logo. Kingston's DataTraveler USB Flash drives all feature advanced Flash controllers and deliver outstanding performance.

The DT Elite offers data transfer rates of up to 24 MB/sec. (read) and 14 MB/sec. (write). Even with encryption, DT Elite's performance levels are not significantly impacted due to the real-time, hardware-based encryption/decryption technology built into the drive.

### 3.2 "Common User" Benchmarks

The following benchmarks were conducted on an Intel D875PBZ motherboard (Intel 875P chipset, 2.4-GHz Pentium® 4 processor, Windows XP Pro + Support Pack 1 installed, 1-GB Kingston HyperX PC3200 memory, and 7200-RPM hard drive). All DataTraveler Flash drives were in new condition and were formatted as FAT32. The benchmark's goal was to measure performance based on typical user scenarios – transferring different kinds and sizes of files from a computer to the DataTraveler Flash drives (utilizing public zones in the DT II, DT II Plus, and DT Elite Flash drives), reading them back, and then deleting the files. The stopwatch approach was used to measure the elapsed time, which was rounded to the closest second.

Note: These benchmarks should be used only as a guide to performance. Many factors, such as the performance level and configuration of the host computer hardware, the Operating System of the host computer and how it's configured, the USB connection speed, and the actual number of files and their sizes may affect benchmark results. In addition, ongoing product improvements may also improve DataTraveler performance.

The DataTraveler drives tested are abbreviated as:

| | |
|---|---|
| DT | = DataTraveler |
| DT II | = DataTraveler II |
| DT II Plus | = DataTraveler II Plus |
| DT Elite | = DataTraveler Elite |

### 3.2.1 Large Directory/Large Number of Files Benchmarks

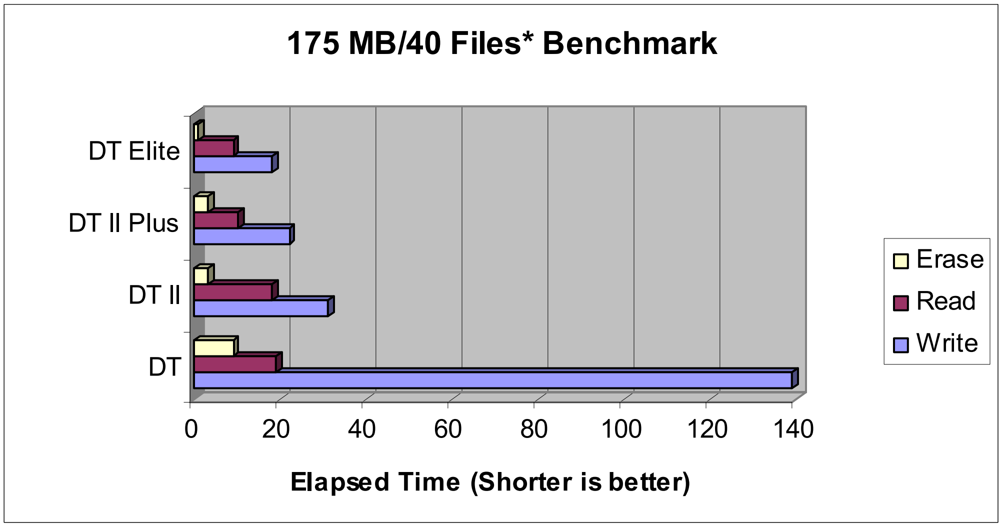
The following three benchmarks utilize large-sized directories with many files to show the performance scalability of DataTraveler Flash drives.

#### 3.2.1.1 175-MB/ 40 Files Benchmark

A 175-MB directory containing 40 files was written to, read from, and erased from the DataTravelers:

| 175-MB,<br>40 Files<br>Benchmark | Write | Read | Erase |
|---|---|---|---|
| DT | 139 | 19 | 9 |
| DT II | 31 | 18 | 3 |
| DT II Plus | 22 | 10 | 3 |
| DT Elite | 18 | 9 | 1 |

Elapsed time (measured in seconds)



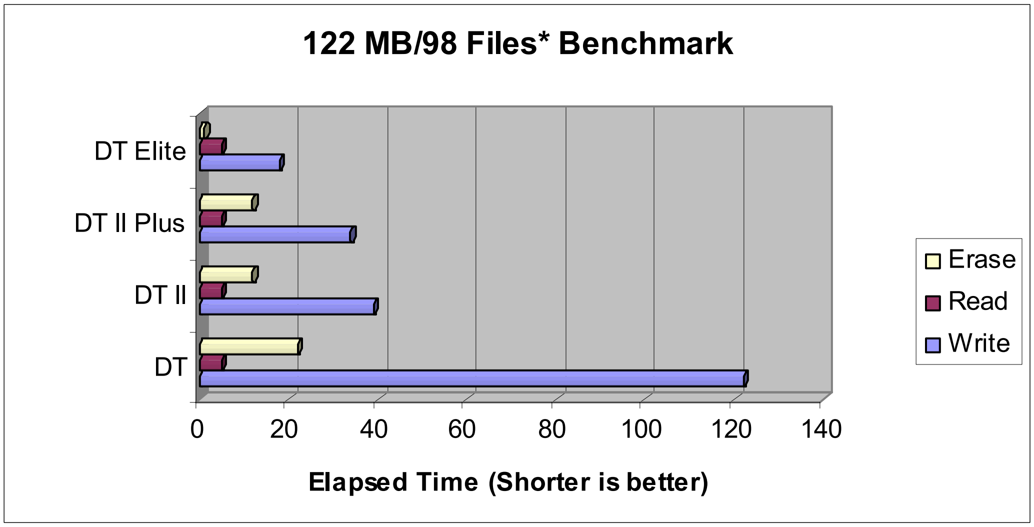
* Files used are PowerPoint files varying in size from 15 KB to almost 21 MB.

### 3.2.1.2 122-MB/98 Files Benchmark

In this benchmark, a 122-MB directory containing 98 files was written to, read from, and erased from the DataTravelers:

| 122-MB,<br>98 Files<br>Benchmark | Write | Read | Erase |
|---|---|---|---|
| DT | 122 | 5 | 22 |
| DT II | 39 | 5 | 12 |
| DT II Plus | 34 | 5 | 12 |
| DT Elite | 18 | 5 | 1 |

Elapsed time (measured in seconds)



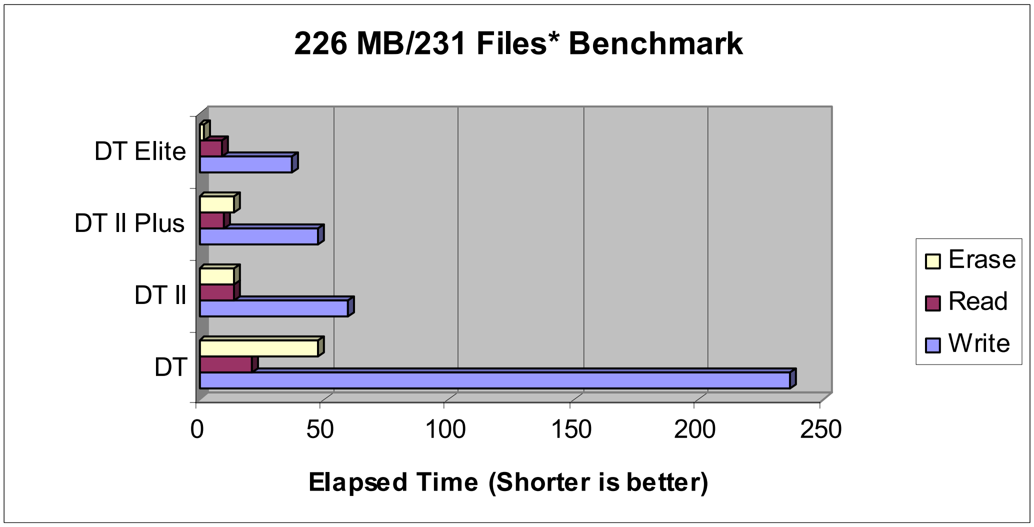
* Files used are JPEG picture files from a 3.3 mega pixel digital camera. File sizes vary from 475 KB to 2.6 MB.

### 3.2.1.3 226-MB/231 Files Benchmark

In this benchmark, a 226-MB directory containing 231 files was written to, read from, and erased from the DataTravelers:

| 226-MB,<br>231 Files<br>Benchmark | Write | Read | Erase |
|---|---|---|---|
| DT | 237 | 21 | 48 |
| DT II | 60 | 14 | 14 |
| DT II Plus | 48 | 10 | 14 |
| DT Elite | 37 | 9 | 2 |

Elapsed time (measured in seconds)

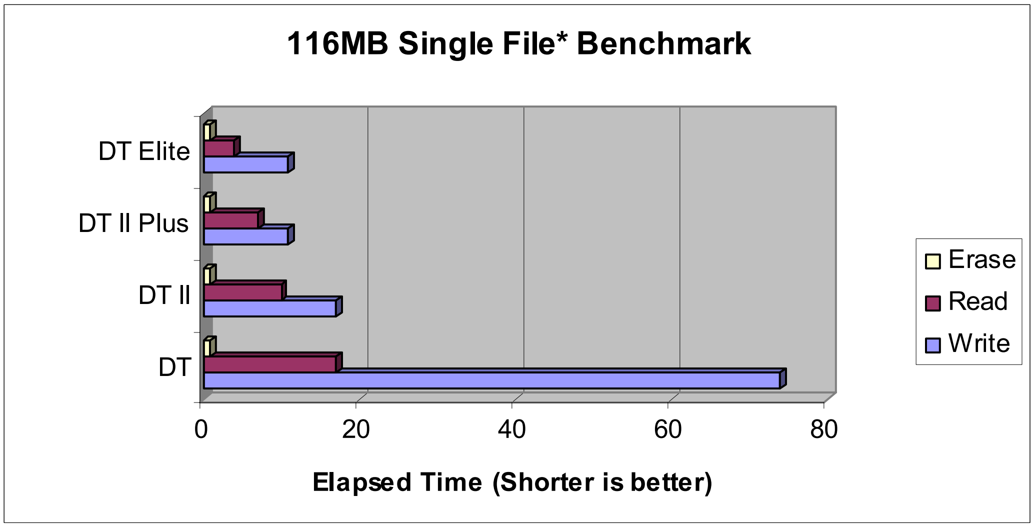


* Files used are JPEG picture files from a 3.3 mega pixel digital camera. File sizes vary from 475 KB to 2.6 MB.

For this benchmark, a single 116-MB file was written to, read from, and erased from the DataTravelers:

| **116-MB File Benchmark** | **Write** | **Read** | **Erase** |
|---|---|---|---|
| **DT** | 74 | 17 | 1 |
| **DT II** | 17 | 10 | 1 |
| **DT II Plus** | 11 | 7 | 1 |
| **DT Elite** | 11 | 4 | 1 |

Elapsed time (measured in seconds)



* File used is a 116 MB audio/video VOB file.

### 3.2.3 DT Elite Encryption/Decryption Performance Benchmark

The175-MB/ 40-Files benchmark was used to test the DT Elite's AES-128 encryption/decryption performance.

| **AES-128 Benchmark** | **Write** | **Read** | **Erase** |
|---|---|---|---|
| **Public Zone (no encryption)** | 18 | 7 | 1 |
| **Privacy Zone (with AES-128 encryption)** | 18 | 7 | 1 |

As expected, there are *absolutely* no performance compromises resulting from the DT Elite's hardware-based AES-128 encryption/decryption.

## 4.0 Conclusion

Kingston's DataTraveler Elite represents the state-of-the-art, advanced security, high-performance Flash drive. It is ideally suited for business organizations as well as advanced consumers seeking the advanced security of hardware AES encryption and high-performance USB 2.0 interface.