

DataTraveler Vault and DataTraveler Vault – Privacy Edition

*Дополнительная безопасность и высокая эффективность.
Белые страницы.*

*Авторизованный перевод статьи «Advanced Security and High Performance White Paper»,
© 2008 Kingston Technology Corporation,*

Введение

Появившиеся на рынке USB Flash - накопители **Kingston's® DataTraveler Vault** ("DT Vault" или просто "DTV") и **DataTraveler Vault - Privacy Edition** ("DT Vault - Privacy" или просто "DTVP") портативны, удобны и просты в использовании. DTV и DTVP сочетают высокую скорость работы с двумя уровнями безопасности и являются одними из наиболее приемлемых USB Flash - накопителей для Windows® - систем.

Данный анонс предоставляет подробную информацию о принятых технических решениях и системе безопасности DTV и DTVP USB накопителей.

DT Vault и DT Vault - Privacy Edition (Специальная разработка для обеспечения конфиденциальности информации)

Система обеспечения безопасности хранимой информации является главной особенностью инженерных решений, принятых в DTV и DTVP накопителях. Надёжность DTV и DTVP накопителей базируется на двухуровневом механизме безопасности, функции аутентификации пользователя, аппаратном шифровании конфиденциальных данных, хранящихся в защищённой зоне Flash-накопителя. С целью повышения безопасности хранящейся информации оба накопителя имеют по встроенному контроллеру с функциями шифрования и расшифровывания.

Основное различие между DTV и DTVP заключается в том, что DTV предполагает наличие зоны, где размещаются видимые и общедоступные файлы. В DTVP не предусмотрены общедоступные зоны. Вся информация зашифрована и невидима до тех пор, пока пользователем не введен верный пароль доступа. Кроме того, накопители DTVP позволяют применять достаточно сложные пароли - длиной от 6 символов, с

возможностью сочетания верхнего и нижнего регистров, алфавитных, числовых и специальных символов. Применение сложных паролей, в сочетании с ограничением попыток последовательного ввода неправильного пароля позволяет применять DTVP для защиты как корпоративной, так и личной конфиденциальной информации.

Аутентификация пользователя

Для активации функции защиты DTV накопителя, пользователю необходимо создать защищенную (зашифрованную) зону. DTV накопитель поставляется с памятью в виде единой общедоступной зоны и вся информация, хранящаяся в ней, может быть просмотрена на любом компьютере. Пользователь в DTV сам создает защищенную зону с помощью программы "DTVaultLock".

DTVP накопители не предусматривают наличие общедоступной зоны и поставляются только со 100 процентной защищенной зоной. Кроме того, DTVP накопители не содержат программу "DTVaultLock" и автоматически активируют программу для ввода пароля доступа к памяти накопителя.

Общедоступные и защищенные зоны на DTV и DTVP накопителях

Пользователь в DTV создает защищенную зону для безопасного хранения информации с помощью программы "DTVaultLock". Данная программа обеспечивает защиту и доступ к информации в операционной среде Windows.

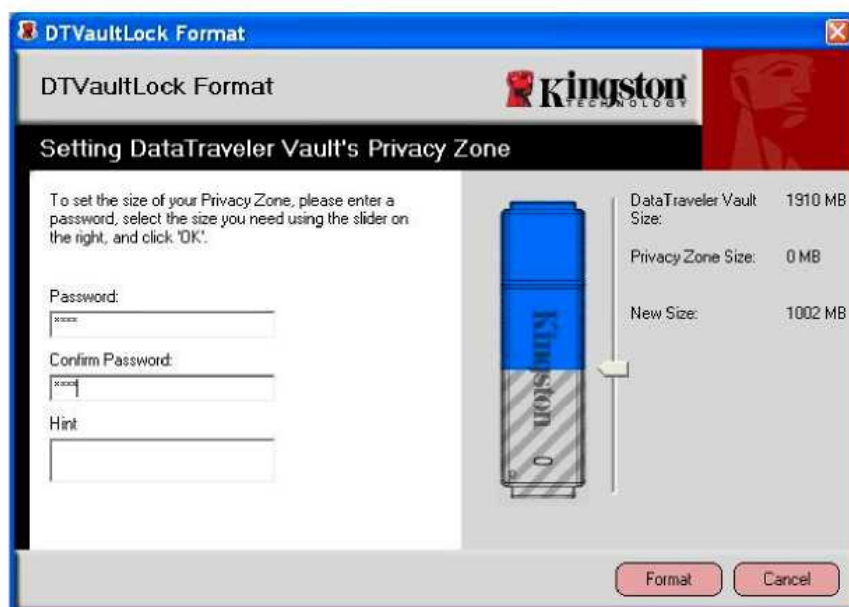


Рис. 1. Изменение размеров зон с помощью "DTVaultLock"

Пользователь с помощью этой программы задаёт пароль доступа к защищенной зоне (где и предполагается хранение конфиденциальной

информации), являющейся областью на накопителе. Данный пароль хранится в DTV в зашифрованном виде, что делает практически невозможным его вскрытие. Общедоступные и защищенные зоны определяются пользователем, как правило, при первичном использовании DTV накопителя. При необходимости принятые размеры зон можно изменить, с помощью программы "DTVVaultLock", как показано на рисунке 1.

После создания защищенной зоны вся конфиденциальная информация, хранящаяся в ней, подвергается шифрованию с применением стандарта AES-256 (Advanced Encryption Standard). При каждом подключении DT Vault к компьютеру программа "DTVVaultLock" обеспечивает подключение к защищенной зоне только после ввода правильного пароля (рис.2).

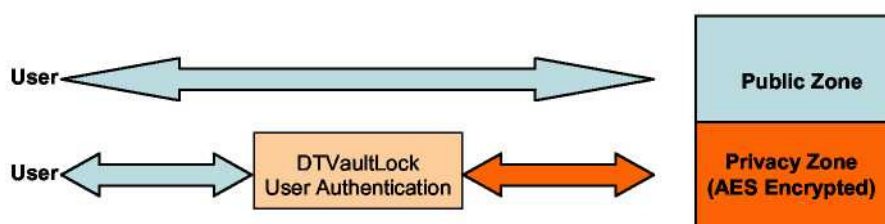


Рис. 2. Защищенная зона может быть открыта только после ввода правильного пароля доступа.

В DTV после последовательного ввода 10 неверных паролей защищенная зона блокируется, в результате чего доступно единственно возможное действие отформатировать накопитель и, тем самым, уничтожить ключ шифрования всю зашифрованную информацию.

DTVP накопитель предназначен исключительно для создания и работы только с защищенной зоной, поэтому реализация общедоступной зоны невозможна. При вводе верного пароля, пользователь получает доступ ко всем файлам, хранящимся в защищенной зоне. DTVP аналогично DTV блокирует защищенную зону после 10 последовательных попыток ввода неправильного пароля.

Шифрование информации в DTV и DTVP

Криптография это наука о шифровании и расшифровывании данных. Как правило, открытая (незашифрованная, незащищенная) информация или файлы преобразуются с помощью программного обеспечения или аппаратных средств в зашифрованный файл. В DTV и DTVP применена технология шифрования, основанная на стандарте AES-256.

Advanced Encryption Standard (AES-256)

AES-256 стандарт шифрования был принят Национальным институтом стандартов и технологий (NIST) в 1997 году. В этом стандарте один и тот же

ключ используется как для шифрования информации, так и для расшифровывания. Ключом является определенная последовательность, сформированная контроллером на основании выбранного пароля. Попытка расшифровывания информации без использования принятого ключа приведет к получению нечитаемой кодовой комбинации.

Аппаратное шифрование защищенных зон в DTV и DTVP

Функции шифрования и расшифровывания на основе стандарта AES реализуются непосредственно на DTV или DTVP во Flash памяти контроллера.

Применительно к DTV, запись информации в общедоступные зоны, производится без шифрования. Чтобы получить доступ к защищенной зоне, пользователь должен использовать программу "DTVVaultLock" и ввести верный пароль. После этого, пользователь получает доступ к работе с информацией в защищённой зоне. В DTVP программа ввода пароля запускается автоматически и после ввода верного пароля пользователь получает доступ к хранящимся расшифрованным данным. При записи информации в защищенные зоны DTV или DTVP она шифруется контроллером по стандарту AES в режиме реального времени и запоминается. Аналогично происходит процесс расшифровывания информации. Без данных уникального для каждого пароля 256-битный ключа, генерируемого генератором случайных чисел, зашифрованные данные практически невозможно расшифровать.

Программное обеспечение шифрования с помощью компьютера

Шифрование информации может производиться и с помощью компьютера (рис. 3)

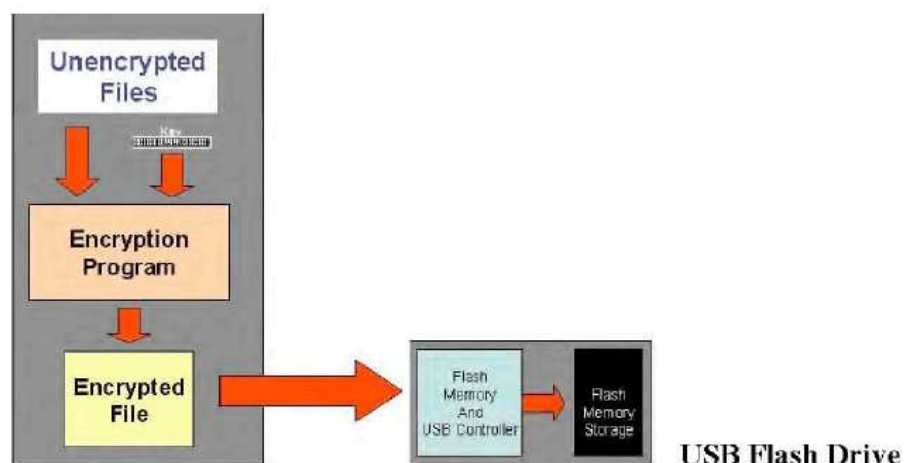


Рис. 3. Шифровании с помощью компьютера.

В этом случае пользователь должен запустить на компьютере программу для шифрования файлов. Если файл зашифрован, то он может

быть скопирован на USB Flash-накопитель. При запуске программы на компьютере, процессы шифрования и расшифровывания занимают достаточно значительные ресурсы процессора и снижают общую производительность системы.

Шифрование файлов с помощью контроллеров DTV и DTVP

Шифрование и расшифровывание по стандарту AES выполняются в DTV и в DTVP аппаратно - контроллером и не используют ресурсы компьютера. Кроме того, применение аппаратных средств шифрования не позволяет выявить данные пароля на компьютере, так как они в нем не хранятся, что значительно повышает уровень безопасности. Сравнительные характеристики DTV и DTVP и иных накопителей представлены в таблице ниже.

Сравнительные характеристики DTV / DTVP с другими продуктами.

Параметры	Характеристики DTV и DTVP с аппаратным шифрованием	Характеристики USB устройств с программным шифрованием
Лимит на количество неправильно введённых паролей	Есть	Редко
Продвинутое шифрование пароля	Есть	Различается у разных моделей
AES сопроцессор	Есть	Нет
Шифрование данных на компьютере	Нет	Да
Ключ AES содержится в компьютере или сети	Нет	Да
Понижение производительности компьютера	Нет	Да

Совместимость с имеющимися Операционными системами:

Накопители DTV и DTVP сертифицированы как Hi-Speed USB 2.0 накопители. Ниже представлена таблица, иллюстрирующая возможности DTV и DTVP в поддержке различных операционных систем:

ОС	DTVP	DTV
Windows	Vista; 2000 SP3, 4; XP SP1, 2	Vista; 2000 SP4; XP SP1, 2, 3
Mac OS 10.3.x и выше / Linux Kernel 2.6 и выше	Нет	Да (действия с файлами ВОЗМОЖНЫ ТОЛЬКО В общедоступной зоне)

DTV и DTVP соответствуют требованиям Криптографического положения Министерства торговли Соединенных Штатов, Бюро по вопросам промышленности и безопасности: регулирование шифрования.

Характеристики DTV и DTVP

В Кингстон DTV и DTVP USB Flash накопители включен Hi-Speed USB 2.0 контроллер, вследствие чего обеспечивается высокий уровень безопасности без снижения быстродействия даже при выполнении операций по шифрованию или расшифровыванию информации. Скорости передачи данных и степень защищённости накопителей Kingston DataTraveler представлены в таблице ниже.

Скорость передачи данных и функции безопасности Kingston's® DataTraveler

Модель	Скорость чтения*	Скорость записи*	Поддержка общедоступной/защищённой зоны	Уровень защиты
DataTraveler Vault	24МБ/сек	10МБ/сек	Есть	Да (Аппаратная AES-256)
DataTravelerVault-Privacy Edition	24МБ/сек	10МБ/сек	Только защищённая зона	Да (Аппаратная AES-256)
DataTraveler 400	15МБ/сек	7МБ/сек	Есть	Нет
DataTraveler II	11МБ/сек	7МБ/сек	Есть	Нет
DataTraveler	5МБ/сек	1.5МБ/сек	Нет	Нет

* Скорость может изменяться в зависимости от параметров компьютера и величины файлов.

Hi-Speed USB 2.0 интерфейс

Скорость интерфейса USB при подключении к различным компьютерам варьируется, следовательно, изменяется и быстродействие подключаемых устройств. Более подробно информация представлена в руководстве Кингстон Flash накопители на http://www.kingston.com/products/pdf_files/FlashMemGuide.pdf.

DTV и DTVP обеспечивают скорость передачи данных до 24 МБ/сек для чтения и 10 МБ/сек при записи (15 МБ/сек скорость чтения для файлов размером более 1GB).

Механическую защиту накопителям придаёт водостойкое титановое покрытие. Водостойкость подтверждена Международной электротехнической комиссией (МЭК) 60529 IPX8.

Заключение

Kingston DataTraveler Vault и DataTraveler Vault - Privacy Edition являются представителями нового высокоскоростного, защищенного поколения USB Flash накопителей. Они идеально подходят для современных потребителей, заботящихся о безопасности собственной конфиденциальной информации.