

Электронный ключ «SecureToken-337F»



Электронный ключ «SecureToken-337F» — это два устройства в одном корпусе: электронный ключ «Secure Token-337» и FLASH-память с логическими дисками для хранения любых данных пользователя.

«SecureToken-337F» полностью совместим с электронным ключом «SecureToken-337», применяется для защищенного хранения и использования ключей электронной цифровой подписи (ЭЦП) налоговой службы Украины, ключей АЦСК государственных и других организаций, в банковских и корпоративных системах, интернет-банкинге и т.п. Выполняет функции формирования и проверки ЭЦП, шифрования, аутентификации, хранения секретной (ключевой) информации.

«SecureToken-337F» может использоваться для хранения любых данных пользователя с защитой от несанкционированного доступа. Поддерживает два типа дисковых массива – открытый и защищенный, общим объемом до 32 Гбайт. Все данные на защищенном носителе хранятся в зашифрованном виде.

Хранение ключей и выполнение криптографических операций реализовано в смарт-чипе компании NXP Semiconductors P5CC037, который используется в «SecureToken-337» (экспертное заключение ГСССЗИ Украины №05/02/02-810 от 11.03.2013 г.).

Технические характеристики «SecureToken-337»:

- генерация и хранение ключевой информации согласно ДСТУ 4145-2002 (длина ключа – 163-509 бит) и RSA (длина ключа – 512-2048 бит);
- шифрование/расшифрование электронных документов согласно ДСТУ ГОСТ 28147:2009, DES, 3-DES, AES;
- формирование и проверка ЭЦП согласно ДСТУ 4145-2002 (длина ключа – 163-509 бит) и RSA (длина ключа – 512-2048 бит);
- вычисление хеш-функций согласно ГОСТ 34.311-95, MD5, SHA;
- реализация схемы аутентификации согласно ISO 9798-3;
- объем памяти 36 Кбайт.

Технические характеристики FLASH-памяти:

- объем памяти: 4, 8, 16 или 32 Гбайт;
- скорость чтения/записи данных на открытом диске, не менее 5 Мбайт/с.

Скорость чтения/записи данных на защищенном диске и алгоритмы шифрования:

Алгоритм шифрования данных во FLASH-памяти	ДСТУ ГОСТ 28147:2009	AES	RC5
Длина ключа, бит	256	128	128
Скорость чтения/записи данных, не менее, Мбайт/с	0,4	0,8	1,7

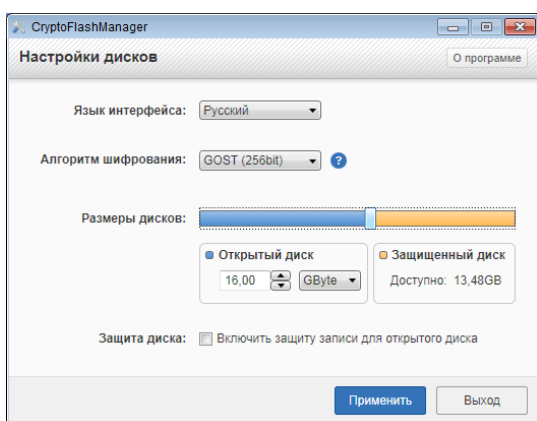
Поддерживаемые интерфейсы и стандарты:

- USB 2.0 High-speed;
- Windows PC/SC;
- Microsoft CCID;
- USB Mass Storage.

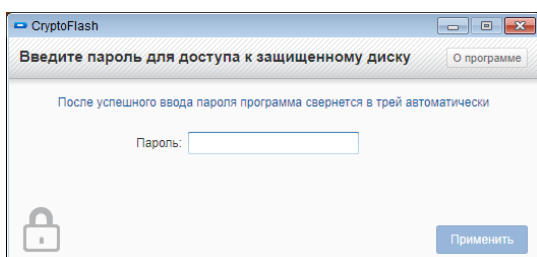
«SecureToken-337F» поддерживает работу со следующими операционными системами: Windows XP/2003/2008/Vista/7/8, Linux, Mac OS. Электронный ключ «SecureToken-337F» поставляется в комплекте с программным обеспечением «**CryptoFlash**».

Программное обеспечение «CryptoFlash»

Программное обеспечение «CryptoFlash» предназначено для управления доступом к данным, находящимся во FLASH-памяти электронного ключа «Secure Token-337F», и состоит из двух утилит «CryptoFlashManager» и «CryptoFlash».



Утилита «CryptoFlashManager» предназначена для управления объёмами открытого и защищенного дисков, выбора алгоритма шифрования для защищенного диска и управления защитой от изменения/удаления файлов, находящихся на открытом диске.



Утилита «CryptoFlash» предназначена для создания, удаления, открытия и извлечения закрытого диска, установления и изменения пароля доступа к защищенному диску.

Программное обеспечение «CryptoFlash» поддерживает работу со следующими операционными системами: Windows XP/Vista/7/8, Mac OS 10.6 и выше. Для операционных систем Mac OS программное обеспечение поставляется отдельной утилитой «CryptoFlashMac».