Загрузка кода в электронный ключ

Для загрузки кода в электронный ключ первоначально используется **GrdUtil.** При помощи этой утилиты создается дескриптор аппаратного алгоритма типа **Загружаемый код**.

В свойствах алгоритма указывается бинарный файл, который содержит скомпилированный загружаемый код. Этому файлу должен сопутствовать файл bmap, содержащий настройки адресов памяти.

Бинарный файл перед загрузкой должен быть преобразован в файл типа **GCEXE** (Guardant Code executable). Преобразование осуществляется в автоматическом режиме утилитой программирования ключей **GrdUtil.**

При выполнении преобразования **GrdUtil** генерирует ключевые пары:

- **Для зашифрования и расшифрования загружаемого кода**
  Зашифрование производится на открытом ключе, который хранится в маске и не записывается в электронный ключ.
  Расшифрование – на закрытом ключе, который храниться‌ся в файле маски, и в дескрипторе алгоритма, записанногов электронный ключ.

- **Для электронной цифровой подписи загружаемого кода**
  Подписывание производится – на закрытом ключе, который хранится только в маске и не записывается в сам ключ.
  Проверка – на открытом, который будет храниться и в маске, и в дескрипторе алгоритма, который будет записан в ключ.

Перед загрузкой бинарный файл зашифровывается на сеансовом ключе и подписывается ЭЦП. Это гарантирует возможность загрузки кода только разработчиком. При необходимости файл **GCEXE** можно сгенерировать таким образом, чтобы он мог быть загружен только в ключ с указанным ID. Эта возможность полезна для создания адресных обновлений, например – платных.

При записи данных в ключ первоначально записывается дескриптор алгоритма, а уже затем – файл **GCEXE.**

Однажды сгенерированный файл **GCEXE** может быть в дальнейшем записан и в другие ключи, содержащие соответствующие ключи шифрования и подписи. Для этого используется функция GrdCodeLoad().