

Глоссарий

Разработчик – создатель программного продукта; программист, использующий электронные ключи Guardant для защиты и лицензирования своего продукта.

Конечный пользователь – клиент разработчика, покупатель программного продукта, защищенного ключами Guardant.

Маска ключа (образ памяти ключа) – образ памяти ключа, сохраненный в базе данных или файле формата .nsd. Совокупность полей памяти, их структуры и значений, представленная в удобной для восприятия форме.

Аппаратный алгоритм – алгоритм шифрования, выполняющийся в электронном ключе. Неизменяемая часть алгоритма, собственно реализующая функцию шифрования, содержится в микропрограмме ключа. Доступная для изменения часть алгоритма (дескриптор) содержится в EEPROM. Дескриптор состоит из набора флагов и определителя (секретного ключа), которые служат для формирования конкретного вида алгоритма и его свойств. Дескриптор алгоритма является разновидностью защищенной ячейки. В большинстве ситуаций, описанных в документации, под аппаратным алгоритмом подразумевается его дескриптор. Это сделано для простоты понимания, т. к. дескриптор – единственная часть аппаратного алгоритма, которой может управлять разработчик.

Защищенная ячейка – тип поля, защищенного аппаратными запретами на чтение/запись и содержащего набор структурированных для той или иной цели данных. К разновидностям защищенных ячеек относятся дескрипторы аппаратных алгоритмов, таблица лицензий (для сетевых ключей), собственно защищенные ячейки (для хранения произвольных данных) и загружаемый код (только для ключей Guardant Code). К достоинствам ячеек относятся: их защищенность от снятия дампа, наличие сервисов активации/деактивации, доступ к содержимому по паролю, упрощенная адресация по номеру ячейки.

Определитель алгоритма – секретный ключ алгоритма, ключ шифрования, один из основных элементов аппаратного алгоритма.

Дескриптор алгоритма – разновидность защищенной ячейки, содержащая характеристики, режимы использования, а также определитель аппаратного алгоритма.

Коды доступа являются одновременно идентификатором разработчика (общий код), по которому защищенное приложение может найти нужный ему ключ, а также паролями для выполнения различных операций Guardant API с ключом: общий код доступа (показывает принадлежность ключа тому или иному разработчику), секретный код чтения (чтение памяти ключа, выполнение аппаратных алгоритмов, обращение к защищенным ячейкам), секретный код записи (запись данных в память ключа) и секретный мастер-код (выполнение специальных операций с ключом-инициализация памяти, установка запретов и пр.). Уникальный набор кодов доступа присваивается разработчику при первом заказе ключей Guardant и прошивается в каждый ключ. Разработчик вводит эти коды в процессе инсталляции комплекта разработчика и использует их при вызове функций Guardant API.

Электронные ключи с определенными кодами доступа может приобрести только лицо/организация-владелец этих кодов.

Демо-коды – комплект демонстрационных (общеизвестных) кодов доступа для работы с электронным ключом Guardant.