Защита данных

Для защиты данных могут применяться следующие технологии:

1. Шифрование при помощи алгоритма AES128.
2. Электронная подпись при помощи алгоритма ECC160.

В ключ Guardant алгоритмы AES128 и ECC160 попадают при записи лицензии. Каждый из компонентов лицензии содержит уникальный ключ шифрования AES и уникальную ключевую пару для алгоритма ECC. Таким образом отсутствие в лицензии нужного компонента автоматически означает невозможность расшифровки данных и проверки электронной подписи.

AES-шифрование

Аппаратный ключ, как и любое устройство, имеет ограниченную производительность. Маленькие объемы данных можно шифровать и расшифровывать напрямую, используя аппаратный алгоритм AES128, записанный в ключ. А для шифрования и расшифровки больших объемов данных рекомендуется использовать программный механизм шифрования.

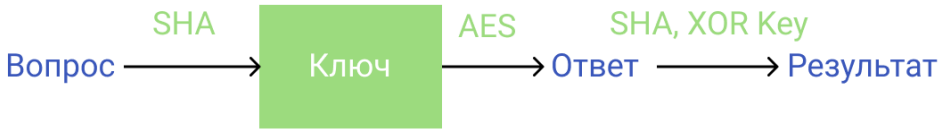
Разработчик может выбрать любой алгоритм (например, AES256). Правильно спроектированный механизм использования данного метода, а также применение средств защиты от реверс-инжиниринга обеспечивают уровень защиты, как при шифровании данных напрямую через аппаратный алгоритм в ключе Guardant.

Главный принцип программного метода: ключ для программного шифрования не хранится в приложении и других файлах, он вычисляется косвенно в процессе работы защищённого приложения при помощи ключей Guardant.

Один из наиболее популярных способов программного шифрования — это таблица Вопросов-Ответов.

Подготовка к защите данных:

1. Запишите в ключ Guardant лицензию хотя бы с одним компонентом.
2. Отдельно сгенерируйте несколько ключей шифрования (например, 5) для выбранного вами программного алгоритма.
3. Сгенерируйте таблицу Вопросов — случайных наборов символов, которые приложение будет отправлять в ключ Guardant для проверки.
4. Вычислите таблицу Ответов. Для этого от каждого Вопроса берётся хеш, потом этот хеш отправляется в ключ Guardant и возвращается уже зашифрованным на AES-алгоритме конкретного компонента лицензии.
5. Вычислите таблицу Результатов. Для этого от каждого ответа берётся хеш и для него выполняется операция xor с ключом программного алгоритма шифрования (каким-то конкретным из сгенерированных на шаге 2).



Защита данных:

1. Зашифруйте защищаемые данные на программных ключах, сгенерированных на шаге 2.
2. Запишите таблицу Вопросов и Результатов в ваше ПО. Обратите внимание, что таблицу Ответов никуда записывать не нужно.

В процессе работы приложения:

1. Приложение отправляет в ключ Guardant хеш случайно выбранного Вопроса.
2. Ключ Guardant шифрует вопрос на аппаратном AES-алгоритме и возвращает Ответ.
3. Приложение хеширует Ответ и выполняет операцию XOR с Результатом, который соответствует заданному Вопросу. Если Вопрос, Ответ и Результат соответствуют друг другу, то на выходе получается ключ для программного алгоритма шифрования, при помощи которого можно расшифровать данные.

   Как только вычисленный ключ шифрования был использован, следует сразу же удалить его из памяти.

Электронная подпись ECC

Подготовка к защите данных:

Запишите в ключ Guardant лицензию хотя бы с одним компонентом.

Защита данных:

1. Подпишите защищаемые данные электронной подписью при помощи алгоритма ECC160 в ключе Guardant (функция Guardant Licensing API автоматически вычисляет хеш для защищаемых данных и возвращает его подпись).
2. Сохраните полученную подпись в приложении или в памяти ключа.
3. Сохраните в приложении открытый ключ от использованного алгоритма ECC160 (находится в интерфейсе Guardant Station на странице конкретного компонента).

В процессе работы приложения:

Приложение через Guardant Licensing API программно проверяет подпись у защищаемых данных при помощи сохранённой подписи и открытого ключа.