Операции с Guardant SP

Софтверный (программный) ключ – это средство защиты недорогих приложений.

Принцип работы Guardant SP основан на привязке ключа к уникальным характеристикам компьютерных комплектующих, состояние которых на момент активации фиксируется в SP-ключе и далее сверяется с текущими значениями при каждом обращении приложения к ключу.

Механизмы привязки, включая сбор и, в дальнейшем, контроль информации о компьютере, обмен данными с сервером активации, перешифрование файла-контейнера SP-ключа и др., реализованы в драйвере Guardant и являются внутренними. Они полностью прозрачны для пользователя и защищены от внешних воздействий.

Этот факт, а также вынос части логики (проверка серийного номера, выработка уникальных ключей шифрования для SP-ключа с участием контрольных значений комплектующих) на внешний защищенный ресурс – сервер активации – существенно повышает стойкость софтверных ключей и выделяет Guardant SP в ряду аналогичных решений.

В свою очередь, защищаемое приложение привязывается к софтверному ключу при помощи «обычных» технологий Guardant – автоматической защиты и/или Guardant API. Реализация этого участка системы защиты, а также подготовка шаблона возлагается на разработчика приложения.

Программный ключ представляет собой файл-контейнер ***.grdvd**, содержащий (в общем виде):

- ***Образ ключа***: защищенные ячейки, алгоритмы, и другую информацию для защиты приложения
- ***Лицензию***: серийный номер и «весовые» коэффициенты комплектующих компьютера на момент активации SP-ключа
- ***Служебные данные***, необходимые для действий с SP-ключом: активация, деактивация и т. п.

Содержимое SP-ключа зашифровано на алгоритме **AES** и защищено от модификации с использованием **ECC.** Хэши от вычисленных контрольных «весовых» значений комплектующих, к которым осуществляется привязка, участвуют в процессе шифрования файла-контейнера.

Для удобства работы в SP-ключе эмулируется **EEPROM-память** современных аппаратных ключей Guardant (размер области данных, доступных для использования составляет ~4Кбайт), а также обеспечивается совместимость со стандартными механизмами защиты. Т. о., программирование и обращение к софтверному ключу из приложения происходят точно также как и для любого другого ключа Guardant.

Это позволяет записывать в софтверный ключ те же типы полей, что и в аппаратные ключи, и после активации SP-ключа точно также работать с этим полями из защищенного приложения, как при помощи Guardant API, так и автозащиты.

> **Важно!**
> Далее рассматриваются только те аспекты работы с программными ключами, которые непосредственно связаны с созданием и программированием образа SP-ключа.
> Комплексная информация по софтверным ключам содержится в **Руководстве по работе с софтверными ключами Guardant SP** и **Руководстве по работе с сервером активации**.

GrdUtil.exe предоставляет удобные сервисы для работы с SP-ключами, в том числе:

- Создание образа софтверного ключа
- Создание в образе полей различных типов, в том числе:
- Защищенных ячеек и запись в них данных, необходимых для работы защищенного приложения
- Алгоритмов шифрования, для последующего обращения к ним из приложения
- Создание шаблона, в т. ч. защищенного, а также активированного SP-ключа для отладки системы защиты
- Настройка параметров привязки ключа к компьютерным комплектующим

В большинстве ситуаций удобно придерживаться следующего порядка работы с софтверными ключами из интерфейса **GrdUtil:**

1. Создать образ SP-ключа
2. Создать поля нужных типов, записать в них данные и сохранить образ.
3. Задать параметры привязки ключа/приложения к характеристикам компьютера.
4. Создать отладочный ключ
5. Выполнить привязку приложения к отладочному ключу при помощи автозащиты и/или Guardant API.
6. Протестировать работу защищенного приложения с отладочным ключом.
7. Используя ранее созданный образ, создать и растиражировать шаблоны SP-ключей для включения в дистрибутив защищенной программы вместе с серийным номером для активации и мастером активации **GuardantActivationWizard.exe**.

Настройка параметров привязки к компьютеру

Создание отладочного софтверного ключа

Шаблон софтверного ключа представляет собой «заготовку», т. е. запрограммированный согласно выбраной схеме защиты, но не активированный, ключ.

Чтобы создать шаблон софтверного ключа, загрузите нужный образ в ***Редактор***, при необходимости отредактируйте его и выполните команду меню **Ключ | (Операции с Guardant SP) Создать шаблон Guardant SP**.

На экране появится системный диалог сохранения файла шаблона, который позволяет задать имя шаблона (по умолчанию **GrdVD_ Template_год_месяц_число.grdvd**) и директории, где он будет расположен.

После этого сохраненный шаблон можно включить в комплект поставки защищенного приложения вместе с серийным номером и мастером активации **GuardantActivationWizard.exe**.
Защищенный шаблон отличается от обычного тем, что содержимое SP-ключа, активированного на таком шаблоне, невозможно изменить программным способом, включая вызовы функций Guardant API.

Это служит дополнительной защитой при использовании софтверных ключей.

Чтобы создать защищенный шаблон, выполните команду меню **Ключ | (Операции с Guardant SP) Защищенный шаблон Guardant SP**.

В остальном работа с защищенным шаблоном полностью аналогична работе с обычным шаблоном, см. *предыдущий пункт*.

Мастер активации SP-ключей