Guardant®

Система защиты от компьютерного пиратства

Эффективная
защита приложений

Урок 1.4: «привязка»
к ключу, находящемуся у конечного пользователя

© 2010 Компания Актив

Содержание

Введение

Обычной является ситуация, когда конечный пользователь (клиент) обращается к разработчику программного обеспечения за новой версией приложения, защищенного при помощи электронного ключа Guardant.

В ходе данного урока будет показано, как «привязать» новую версию (или новое приложение) к электронному ключу, находящемуся у конечного пользователя – без перезаписи маски в ключе.

Следует отметить, что в зависимости от способа установки автозащиты (с самостоятельным или с автоматическим программированием ключа), порядок действий будет различаться.

Случай с автоматическим программированием ключа проще, так как не требует от разработчика изучения устройства ключа. В этом случае достаточно выбрать пятый пункт в Мастере лицензирования и автозащиты (**Защитить новую версию приложения на основе существующей лицензии**) и, открыв нужный проект лицензирования, следовать указаниям Мастера.

При самостоятельном программировании ключа указанный пункт Мастера недоступен, так как информация о лицензии в соответствующем электронном ключе находится не в составе проекта, а в базе данных утилиты программирования ключей. В ходе урока будут рассмотрены действия, которые необходимо совершить для установки автозащиты в этой ситуации.

Примечание

Данный урок будет полезен и тем, кто привык работать с более ранними версиями комплекта разработчика Guardant. В уроке представлены скриншоты утилит комплекта разработчика версии 5.5, однако все описанные действия могут быть выполнены и с утилитами более ранних (начиная с 4.8) версий МК, с поправкой на различия формулировок сообщений и названий элементов интерфейса.

Используемые термины и обозначения

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 – совокупность структур данных, описывающих содержимое электронного ключа, подлежащих записи внутрь ключа на этапе тиражирования лицензий защищенного приложения.

Проект автозащиты – параметры установки автозащиты, сохраненные в формате Мастера лицензирования и автозащиты.

Проект лицензирования – совокупность параметров установки автозащиты, а также формата и содержания маски ключа, создаваемой Мастером автозащиты в режиме автоматического программирования ключа.

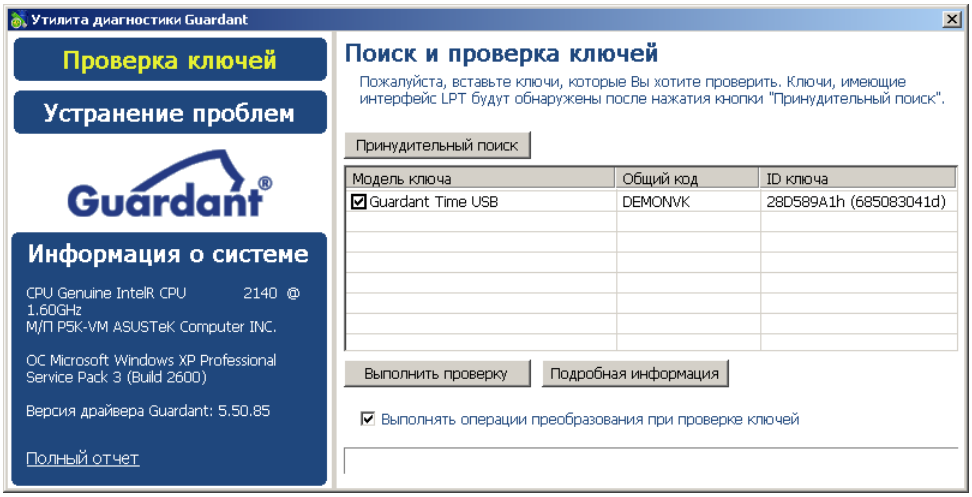
Установка автозащиты

Одним из важных шагов при установке автозащиты является запись в ключ на стороне разработчика маски, соответствующей содержимому ключа, находящегося у конечного пользователя.

Это необходимо, так как маска была сформирована и записана в ключ разработчиком вручную, при помощи утилиты программирования ключей, то есть выполнялась установка автозащиты с **самостоятельным программированием** ключа разработчиком.

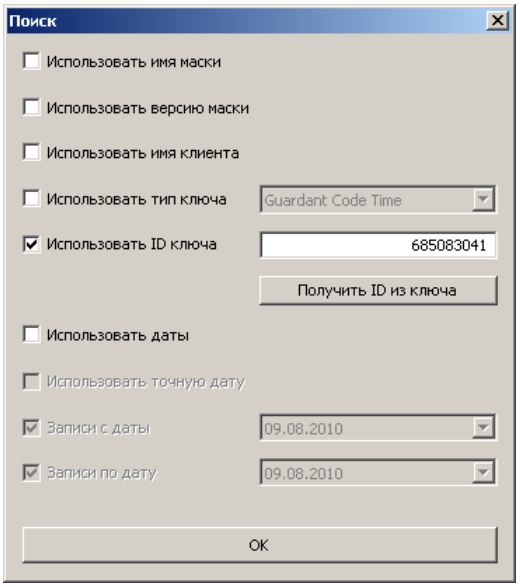
Шаг 0. Определение критериев поиска маски ключа

Поиск маски, соответствующей последнему факту прошивки ключа клиента удобно производить по ID ключа, который нанесен на корпус ключа клиента, а также может быть считан программно при помощи утилиты диагностики Guardant из состава комплекта драйверов (**Панель управления | Драйверы Guardant | Диагностика**).

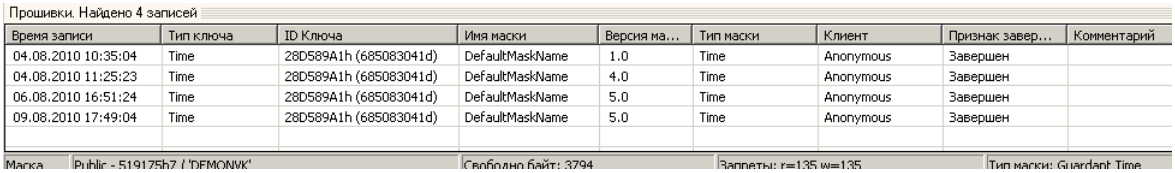


Шаг 1. Поиск маски ключа

В утилите программирования ключей выполним команду меню **База данных | Поиск прошивок ключей**, установив ID ключа клиента в качестве условия поиска:

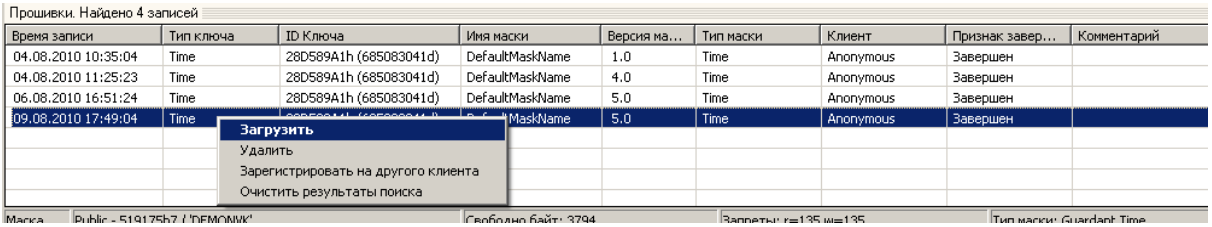


В результате в окне **Прошивки**, расположенном в нижней части утилиты GrdUtil, будет выведена информация о всех фактах программирования ключа с указанным ID:

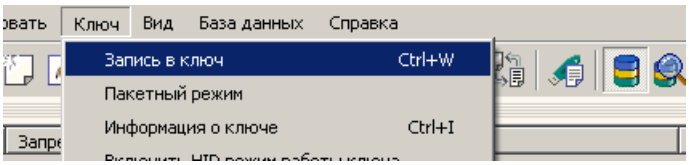


Шаг 2. Запись маски ключа

Загружаем маску, соответствующую последней прошивке ключа



...и записываем ее в любой электронный ключ Guardant подходящей модели:



Подготовка электронного ключа завершена. Можно переходить непосредственно к установке автозащиты.

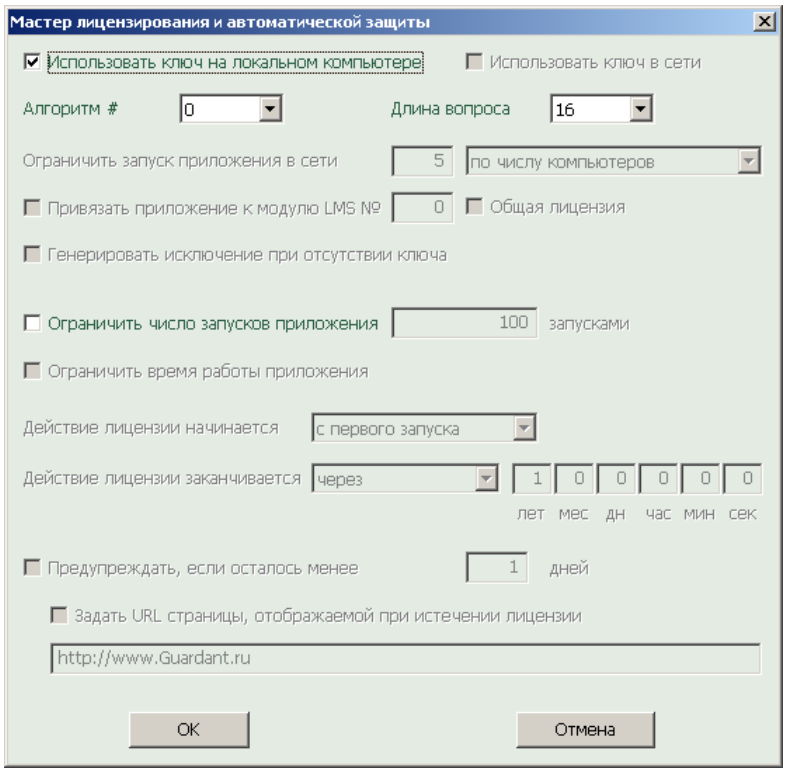
Шаг 3. Создание проекта автозащиты

Для создания проекта автозащиты необходимо воспользоваться шестым пунктом Мастера автозащиты (**Установить автозащиту без программирования ключа**):

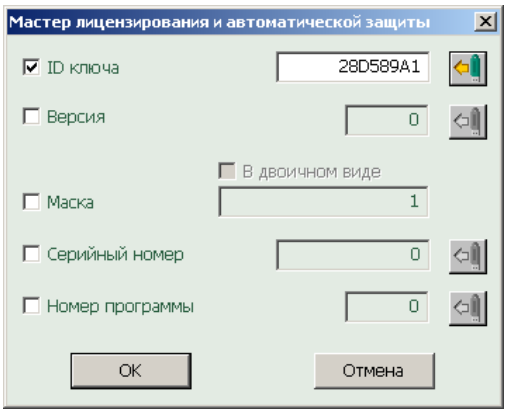
Иногда имеет смысл воспользоваться ранее созданным проектом автозащиты, однако, в указанном случае следует уделить не менее пристальное внимание установке параметров автозащиты.

Шаг 4. Установка параметров автозащиты

Прежде всего, необходимо определиться с **числовым именем** (номером) аппаратного алгоритма, предназначенного для использования автозащитой (диалог **Параметры лицензирования** список **Алгоритм #**). Значение этого параметра должно соответствовать числовому имени симметричного алгоритма ключа конечного пользователя:



Также следует обратить внимание на установку **Параметров поиска ключей**. Необходимо понимать, что, к примеру, при отсутствии привязки к строго определенному электронному ключу (по ID) распространяемая копия защищенного приложения будет доступна всем конечным пользователям, ключи которых содержат аналогичную маску, что может противоречить **политике лицензирования приложений**:



Подробнее об установке остальных параметров автозащиты информацию можно получить в других уроках серии 1.x, а также **документации Guardant**.

Контрольные испытания

После окончания процесса защиты исполняемого файла и до передачи продукта конечному пользователю, рекомендуется провести ряд контрольных испытаний защищенного приложения, в ходе которых проверить:

- Корректность работы приложения в целом
- Корректность работы защищенного функционала приложения
- Устойчивость работы защищенного функционала в различных средах и при различных нагрузках

В результате успеха при проведении контрольных испытаний будет получен готовый для передачи конечному пользователю программный продукт, защищенный на лицензии, находящейся в ключе конечного пользователя

Примечание

При установке привязки по ID ключа (флаг /UI) полноценное тестирование произвести не удастся, так как приложение будет работать исключительно с электронным ключом конечного пользователя. Для проведения тестирования и контрольных испытаний рекомендуется защитить приложение с привязкой к ключу разработчика, после успешного испытания контрольных испытаний, перезащитить его с использованием BAT-файла, изменив значение параметра /UI на ID ключа конечного пользователя.

Заключение

В данном уроке был рассмотрен порядок действий, необходимых для защиты приложения на электронный ключ, находящийся у конечного пользователя – без необходимости перезаписи содержимого ключа.

Перечисленных действий достаточно, если лицензия, записанная в ключ конечного пользователя, актуальна и может быть использована для защиты нового приложения.

В случае, когда срок действия лицензии (либо счетчик числа запусков) истек или необходимо записать в ключ новую лицензию, повторная пересылка электронного ключа также не требуется. Разрешить ситуацию можно при помощи процедуры удаленного обновления ключа (**Trusted Remote Update, TRU**), речь о котором пойдет в одном из следующих уроков.

Дополнительные источники информации

При возникновении вопросов, на которые вам не удалось найти ответа в этом пособии, рекомендуем обратиться к следующим дополнительным источникам информации:

WWW: http://www.guardant.ru

Web-сайт разработчика содержит большой объем справочной информации об электронных ключах Guardant.

Служба технической поддержки:

e-mail: hotline@guardant.ru

тел. +7(495)925-77-90