

РСС-2021

Дистанционное обновление памяти ключа

© 2012 ОАО МЦС «Мосстройцены»

Общее описание технологии

Технология безопасного удаленного обновления предназначена для **обновления памяти ключа**, находящегося у **конечного пользователя** защищенной программы, без передачи электронного ключа разработчику.

Обновление памяти ключа может быть полезно при необходимости:

- Продления срока использования приложения, ограниченного по времени использования или числу запусков
- Активации демо-версии приложения
- Увеличения числа доступных лицензий сетевого приложения
- Обновления версии программы
- Покупки конечным пользователем другого защищенного приложения разработчика – для записи новой лицензии в ключ

Основное достоинство технологии заключается в том, что она **предельно проста**.

Пользователю достаточно иметь утилиту **GrdTRU.exe**, распространяемую в составе дистрибутива защищенного приложения.

В рамках данного урока будет приведен протокол процедуры удаленного обновления ключа, а также будут подробно описаны действия, совершаемые сторонами в процессе удаленного обновления памяти ключа.

Используемые термины и обозначения

Доверенное удаленное обновление (Trusted Remote Update, TRU) – технология безопасного удаленного обновления памяти электронного ключа, исключающая возможность компрометации и/или фальсификации данных.

Протокол удаленного обновления

Процесс удаленного (дистанционного) программирования ключей Guardant состоит из 4 этапов и выглядит следующим образом:

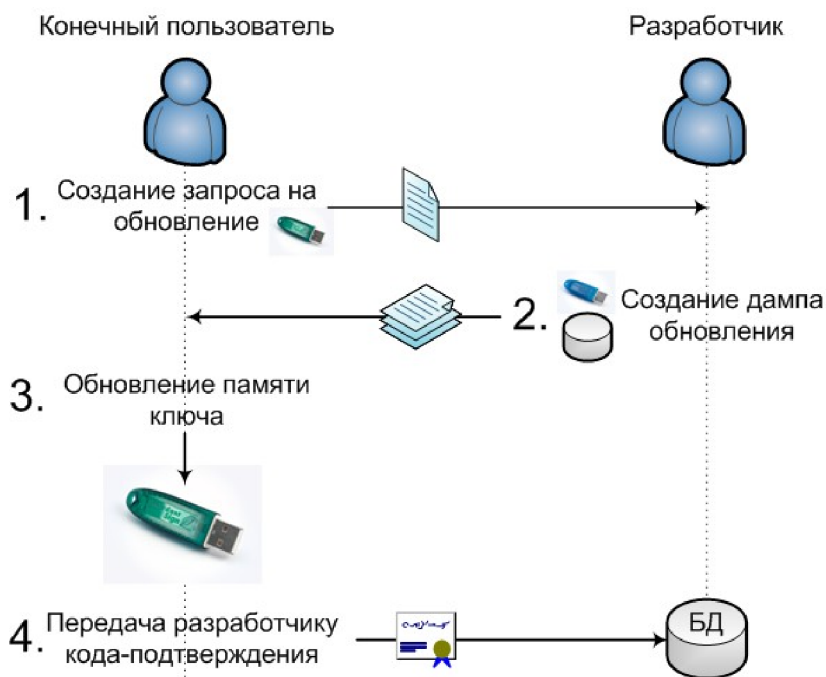


Схема 1. Протокол доверенного удаленного обновления

На 1-м этапе пользователь защищенного приложения генерирует **запрос на обновление памяти** электронного ключа и обращается к разработчику за новой лицензией.

2-й этап происходит на стороне разработчика и включает поиск маски, записанной в ключ пользователя, ее модификацию и генерацию **дампа обновления** памяти для удаленного ключа, а также пересылку дампа конечному пользователю.

3-й этап представляет собой непосредственное обновление памяти ключа (применение дампа обновления), в результате которого пользователь получает **код подтверждения** завершения операции обновления.

4-й этап заключается в получении от пользователя кода подтверждения и фиксации успешного **статуса завершения** операции в базе прошивок.

Безопасность обмена обеспечивается паролем удаленного обновления, записываемого в ключ и сохраняемого в БД прошивок в момент записи маски в ключ. Таким образом, обмен может происходить по открытому каналу связи.

Удаленное обновление

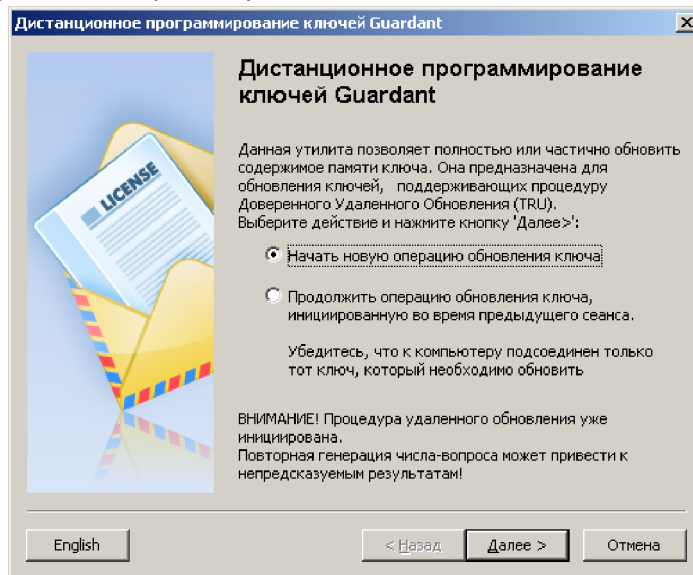
На примере рассмотрим подробнее весь цикл удаленного обновления памяти ключа.

Шаг 1. Создание запроса на обновление

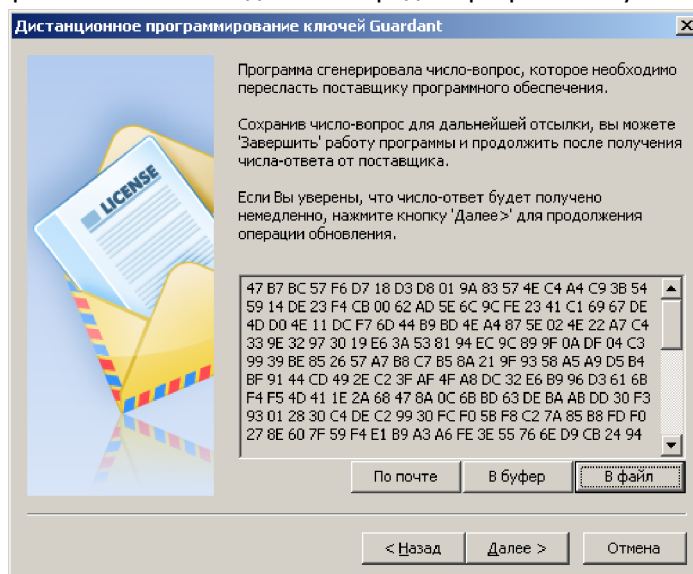
Рассмотрим ситуацию, когда после передачи конечному пользователю ключа и приложения, клиент покупает у разработчика новое приложение, лицензируемое отдельно.

Таким образом, в ключе пользователя необходимо добавить алгоритм, соответствующий лицензии на новое приложение.

Конечный пользователь – с санкции разработчика – при помощи специальной утилиты (**GrdTRU.exe**) начинает процесс удаленного обновления:



Происходит генерация запроса на обновление памяти ключа (т. н. **числа-вопроса**).
Созданный запрос пользователь должен передать разработчику:



В окне диалога предложены три варианта сохранения запроса. При нажатии кнопки **[По почте]** будет автоматически сформировано письмо, во вложении которого будет содержаться файл с запросом. Кнопки **[В файл]** и **[В буфер]** позволяют, соответственно,

сохранить запрос в виде файла, или сохранить его в буфер.

Сохраним запрос в файл. Имя файла, предлагаемое по умолчанию, имеет название вида **question_ID_DATE.txt**. После сохранения числа-вопроса работу утилиты можно завершить (кнопка **[Завершить/Отмена]**).

Примечание

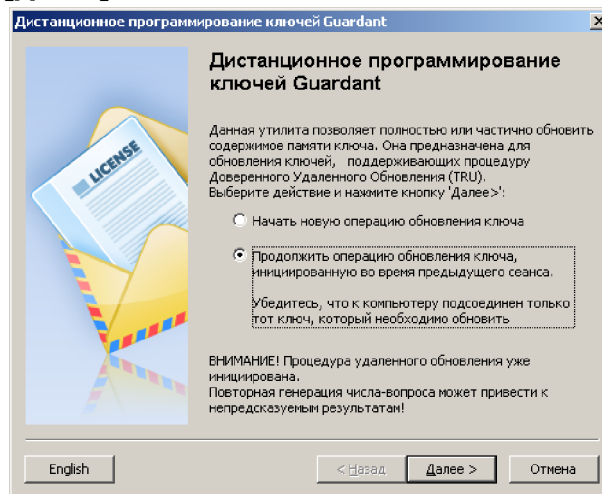
В случае генерации пользователем нескольких запросов на обновление действителен будет последний. Обновление памяти ключа может быть выполнено только на нем.

Шаг 2. Создание дампа обновления

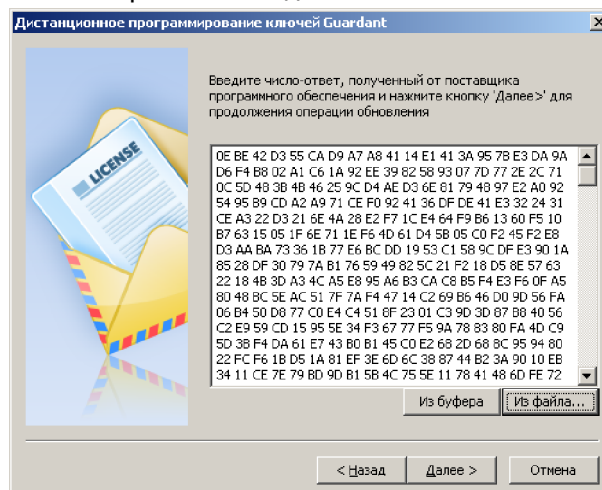
Получив запрос на обновление, разработчик на основании информации полученной из файла формирует дамп обновления ключа и отправляет его конечному пользователю.

Шаг 3. Обновление памяти ключа

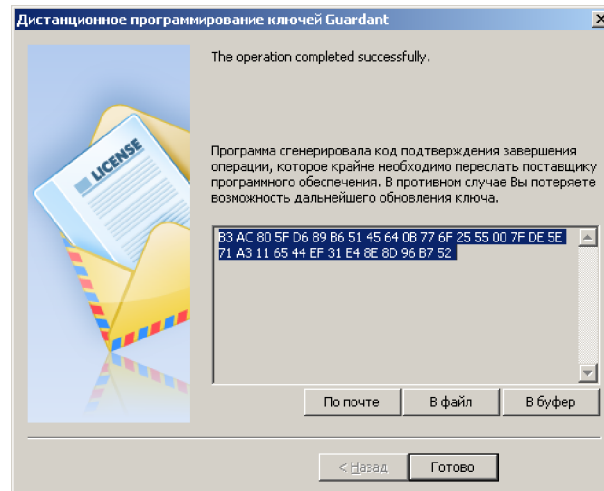
После получения дампа обновления пользователю необходимо снова запустить клиентскую утилиту обновления **GrdTRU**, выбрать пункт **Продолжить операцию обновления ключа** и нажать на кнопку **[Далее]**:



После ввода дампа обновления и нажатия на кнопку **[Далее]** будет произведена операция по обновлению памяти ключа присланными данными.



В случае успешного окончания на экране появится последняя страница мастера с итогами выполнения операции:



В результате успешного обновления памяти ключа утилита **GrdTRU** выдаст код подтверждения, содержащий информацию о результате обновления. Пользователю следует сохранить его и передать разработчику приложения любым удобным способом. Иначе **пользователь потеряет возможность** в дальнейшем производить удаленное обновление.

Шаг 4. Завершение удаленного обновления

После получения кода подтверждения разработчик завершает процедуру обновления, занося в базу данных информацию о результате состоявшегося обновления.