

GrdTRU_ApplyAnswer

Функция(метод) **GrdTRU_ApplyAnswer** производит отправку зашифрованного ответа в ключ для выполнения завершающей фазы удаленного программирования при использовании технологии Trusted Remote Update.

C

```
int GRD_API GrdTRU_ApplyAnswer (
    HANDLE hGrd,
    void *pAnswer,
    DWORD dwAnswerSize
);
```

<i>hGrd</i>	хэндл, через который будет выполнена данная операция. Электронный ключ, к которому "логинится" данный хэндл, должен содержать 128-битный секретный ключ шифрования TRU, прошитый функцией GrdTRU_SetKey на этапе предпродажной подготовки, а также ранее сгенерированное число-вопрос
<i>pAnswer</i>	буфер, содержащий ответ, подготовленный и зашифрованный функцией GrdTRU_EncryptAnswer
<i>dwAnswerSize</i>	длина буфера, содержащего ответ

Возможные ошибки

GrdE_SystemDataCorrupted	Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует)
GrdE_NoQuestion	Число-вопрос не было сгенерировано или было перегенерировано до записи числа ответа
GrdE_InvalidData	Неверный формат данных для удаленного программирования
GrdE_QuestionOK	Число-вопрос уже было сгенерировано, ключ ожидает данных для удаленного программирования
GrdE_UpdateNotComplete	Ошибка при записи данных удаленного программирования. Операция не была завершена
GrdE_InvalidHash	Неверное значение MAC (Message Authentication Code)
	Набор ошибок Guardant API

Функция **GrdTRU_ApplyAnswer** производит отправку зашифрованного ответа, сгенерированного функцией [GrdTRU_EncryptAnswer](#) в ключ для выполнения завершающей фазы удаленного программирования. Ответ представляет собой последовательность команд и набор данных, зашифрованных и защищенных от подмены.

Электронный ключ, в который поступает ответ, проверяет его подлинность и производит расшифровывание данных и команд.

При подтверждении подлинности и правильном расшифровывании данные, которые содержатся в ответе, записываются в память ключа. Если в данном сеансе удаленного программирования производится полное перепрограммирование памяти (изменение количества аппаратных алгоритмов, защищенных ячеек, изменение границ аппаратных запретов чтения/записи), перед записью память ключа инициализируется (см. [GrdInit](#)), производится запись данных, а затем производится установка количества аппаратных алгоритмов, защищенных ячеек и границ аппаратных запретов чтения/записи (см. [GrdProtect](#)). При этом функции [GrdInit](#) и [GrdProtect](#) не вызываются, а выполняются ключом в автономном режиме.

Число-вопрос с момента его генерации не должно изменяться или перегенерироваться. В противном случае весь сеанс удаленного программирования придется повторять заново.

C#

```
public static GrdE GrdTRU_ApplyAnswer(Handle grdHandle, byte[] answer)
```

grdHandle [in]

Тип: [Handle](#)

Нэндл, через который будет выполнена данная операция.

question [in]

Тип: [byte](#) []

Буфер, который содержит ответ, подготовленный и зашифрованный функцией [GrdTRU_EncryptAnswer](#)

Возможные ошибки

GrdE.SystemDataCorrupted	Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует)
GrdE.NoQuestion	Число-вопрос не было сгенерировано или было регенерировано до записи числа ответа
GrdE.InvalidData	Неверный формат данных для удаленного программирования
GrdE.QuestionOK	Число-вопрос уже было сгенерировано, ключ ожидает данных для удаленного программирования
GrdE.UpdateNotComplete	Ошибка при записи данных удаленного программирования. Операция не была завершена
GrdE.InvalidHash	Неверное значение MAC (Message Authentication Code)
	Набор ошибок Guardant API

Метод **GrdTRU_ApplyAnswer** производит отправку зашифрованного ответа, сгенерированного методом [GrdTRU_EncryptAnswer](#) в ключ для выполнения завершающей фазы удаленного программирования. Ответ представляет собой последовательность команд и набор данных, зашифрованных и защищенных от подмены.

Электронный ключ, в который поступает ответ, проверяет его подлинность и производит расшифровывание данных и команд.

При подтверждении подлинности и правильном расшифровывании данные, которые содержатся в ответе, записываются в память ключа. Если в данном сеансе удаленного программирования производится полное перепрограммирование памяти (изменение количества аппаратных алгоритмов, защищенных ячеек, изменение границ аппаратных запретов чтения/записи), перед записью память ключа инициализируется (см. [GrdInit](#)), производится запись данных, а затем производится установка количества аппаратных алгоритмов, защищенных ячеек и границ аппаратных запретов чтения/записи (см. [GrdProtect](#)). При этом методы [GrdInit](#) и [GrdProtect](#) не вызываются, а выполняются ключом в автономном режиме.

Число-вопрос с момента его генерации не должно изменяться или регенерироваться. В противном случае весь сеанс удаленного программирования придется повторять заново.

Java

```
public static GrdE GrdTRU_ApplyAnswer(Handle grdHandle, byte[] answer)
```

grdHandle [in]

Тип: [Handle](#)

Нэндл, через который будет выполнена данная операция.

question [in]

Тип: [byte \[\]](#)

Буфер, который содержит ответ, подготовленный и зашифрованный функцией [GrdTRU_EncryptAnswer](#)

Возможные ошибки

GrdE.SystemDataCorrupted	Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует)
GrdE.NoQuestion	Число-вопрос не было сгенерировано или было регенерировано до записи числа ответа
GrdE.InvalidData	Неверный формат данных для удаленного программирования
GrdE.QuestionOK	Число-вопрос уже было сгенерировано, ключ ожидает данных для удаленного программирования
GrdE.UpdateNotComplete	Ошибка при записи данных удаленного программирования. Операция не была завершена
GrdE.InvalidHash	Неверное значение MAC (Message Authentication Code)
	Набор ошибок Guardant API

Метод **GrdTRU_ApplyAnswer** производит отправку зашифрованного ответа, сгенерированного методом [GrdTRU_EncryptAnswer](#) в ключ для выполнения завершающей фазы удаленного программирования. Ответ представляет собой последовательность команд и набор данных, зашифрованных и защищенных от подмены.

Электронный ключ, в который поступает ответ, проверяет его подлинность и производит расшифровывание данных и команд.

При подтверждении подлинности и правильном расшифровании данные, которые содержатся в ответе, записываются в память ключа. Если в данном сеансе удаленного программирования производится полное перепрограммирование памяти (изменение количества аппаратных алгоритмов, защищенных ячеек, изменение границ аппаратных запретов чтения/записи), перед записью память ключа инициализируется (см. [GrdInit](#)), производится запись данных, а затем производится установка количества аппаратных алгоритмов, защищенных ячеек и границ аппаратных запретов чтения/записи (см. [GrdProtect](#)). При этом методы [GrdInit](#) и [GrdProtect](#) не вызываются, а выполняются ключом в автономном режиме.

Число-вопрос с момента его генерации не должно изменяться или регенерироваться. В противном случае весь сеанс удаленного программирования придется повторять заново.