

# GrdTRU\_EncryptAnswer

Функция(или метод) **GrdTRU\_EncryptAnswer** предназначены для подготовки данных (ответа) при использовании технологии Trusted Remote Update. Эта функция(или метод) не подходит для ключей Guardant Code, при работе с которыми нужно использовать функцию(метод) [GrdTRU\\_EncryptAnswerEx](#).

C

```
int GRD_API GrdTRU_EncryptAnswer(
    HANDLE hGrd,
    DWORD dwAddr,
    DWORD dwLng,
    void *pData,
    void *pQuestion,
    DWORD dwAlgoNum_GSII64,
    DWORD dwAlgoNum_Hash64,
    void *pAnswer,
    DWORD *pdwAnswerSize
);
```

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>hGrd</i>             | хэнгл, через который будет выполнена данная операция. В ключ, соответствующий этому хэнглу должен быть записан тот же секретный ключ, что и в удаленном ключе. Также ключ должен содержать алгоритмы GSII64 и HASH64, в качестве определителей которых используется секретный ключ                                                                                                                                                                                  |
| <i>dwAddr</i>           | стартовый адрес (в системе адресации SAM) в памяти удаленного ключа, по которому будет производиться запись данных                                                                                                                                                                                                                                                                                                                                                  |
| <i>dwLng</i>            | длина буфера данных, которые должны быть записаны в удаленный ключ                                                                                                                                                                                                                                                                                                                                                                                                  |
| <i>pData</i>            | буфер, содержащий данные для записи в удаленный ключ                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>pQuestion</i>        | указатель на буфер, содержащий расшифрованное 64-битное число-вопрос                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>dwAlgoNum_GSII64</i> | номер алгоритма типа GSII64, который будет использоваться для зашифрования ответа. Определителем алгоритма должен быть тот же секретный 128-битный ключ, что был записан операцией <a href="#">GrdTRU_SetKey</a> в удаленный ключ                                                                                                                                                                                                                                   |
| <i>dwAlgoNum_Hash64</i> | номер алгоритма типа HASH64, который будет использоваться для вычисления хэш-функции для проверки подлинности ответа. Определителем алгоритма должен быть тот же секретный 128-битный ключ, что был записан операцией <a href="#">GrdTRU_SetKey</a> в удаленный ключ                                                                                                                                                                                                |
| <i>pAnswer</i>          | указатель на буфер, в который будет помещен зашифрованный ответ. Под буфер рекомендуется выделять памяти не менее $dwLng * 3 + 128$ байт                                                                                                                                                                                                                                                                                                                            |
| <i>pdwAnswerSize</i>    | указатель на переменную типа <b>DWORD</b> , которая при вызове должна содержать значение длины буфера <i>pAnswer</i> . После вызова в нее будет записан размер буфера <i>pAnswer</i> , использованный для размещения ответа. Если изначально размер буфера был меньше необходимого, функция возвращает код ошибки <a href="#">GrdE_InvalidArg</a> . В таком случае это значение необходимо использовать в качестве минимального размера при выделении нового буфера |

### Возможные ошибки

|                                          |                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">GrdE_AlgoNotFound</a>        | Аппаратный алгоритм с заданным номером не существует                                      |
| <a href="#">GrdE_CRCErrorFunc</a>        | Ошибка при вызове аппаратного алгоритма                                                   |
| <a href="#">GrdE_InactiveItem</a>        | Аппаратный алгоритм деактивирован, обращение к нему невозможно                            |
| <a href="#">GrdE_SystemDataCorrupted</a> | Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует) |
| <a href="#">GrdE_NoQuestion</a>          | Число-вопрос не было сгенерировано или было регенерировано до записи числа ответа         |
| <a href="#">GrdE_InvalidData</a>         | Неверный формат данных для удаленного программирования                                    |
| <a href="#">GrdE_QuestionOK</a>          | Число-вопрос уже было сгенерировано, ключ ожидает данных для удаленного программирования  |
| <a href="#">GrdE_UpdateNotComplete</a>   | Ошибка при записи данных удаленного программирования. Операция не была завершена          |
| <a href="#">GrdE_InvalidHash</a>         | Неверное значение MAC (Message Authentication Code)                                       |
|                                          | <a href="#">Набор ошибок Guardant API</a>                                                 |

Функция **GrdTRU\_EncryptAnswer** предназначена для подготовки данных (ответа) при использовании технологии Trusted Remote Update.

При подготовке ответа функция **GrdTRU\_EncryptAnswer** генерирует зашифрованный ответ. Этот ответ представляет собой последовательность команд и набор данных. Расшифровка ответа, проверка его подлинности, последующее выполнение команд и запись данных *pData* по адресу *dwAddr* производится непосредственно микропрограммой внутри удаленного электронного ключа.

Поскольку кроме данных *pData*, которые должны быть записаны в память удаленного ключа, ответ содержит команды и другую служебную информацию, длина ответа *pdwAnswerSize* получается больше, чем длина данных *dwLng*. Соответственно для размещения ответа *pAnswer* необходимо зарезервировать памяти больше, чем *dwLng*.

Функция проверяет, достаточно ли памяти выделено для ответа, и если размер буфера недостаточен, возвращается код ошибки [GrdE\\_InvalidArg](#). При этом в переменную *pdwAnswerSize* записывается минимальный размер буфера для генерации ответа. Это значение необходимо учитывать при повторном выделении памяти для буфера.

Шифрование ответа производится аппаратным алгоритмом типа GSII64 с номером *dwAlgoNum\_GSII64*. На момент шифрования этот алгоритм должен быть создан в ключе, находящемся у разработчика. В качестве определителя должен использоваться секретный 128-битовый ключ, который был сгенерирован и прошит в ключ удаленного пользователя при предпродажной подготовке функцией [GrdTRU\\_SetKey](#) для ключа с ID, равным *dwID*. При использовании GRDUTIL этот ключ берется из базы данных или из соответствующей маски электронного ключа.

Для последующей проверки подлинности ответа производится вычисление хеш-функции аппаратным алгоритмом типа Hash64 с номером задаваемым через параметр *dwAlgoNum\_Hash64*. На момент вычисления этот алгоритм должен быть создан в ключе, находящемся у разработчика. В качестве определителя должен использоваться секретный 128-битовый ключ, который был сгенерирован и прошит в ключ удаленного пользователя при предпродажной подготовке функцией [GrdTRU\\_SetKey](#) для ключа с ID равным *dwID*. При использовании GRDUTIL этот ключ берется из базы данных.

Рабочий ключ, находящийся у разработчика, не обязательно должен быть инициализирован также функцией [GrdTRU\\_SetKey](#) с секретным ключом, таким же как у удаленного пользователя. Все преобразования делаются на заранее запрограммированных алгоритмах, номера которых указываются в параметрах указываемых в параметрах *dwAlgoNum\_GSII64* и *dwAlgoNum\_Hash64*.

## C#

```
public static GrdE GrdTRU_EncryptAnswer(Handle grdHandle, uint addr, byte[] data, byte[] question,
    int algNum_GSII64, int algNum_HashS3, out byte[] answer)
```

*grdHandle* [in]

Тип: [Handle](#)

Нэндл, через который будет выполнена данная операция.

*addr* [in]

Тип: uint

Стартовый адрес (в системе адресации SAM) в памяти удаленного ключа, по которому будет производиться запись данных.

*data* [in]

Тип: byte [ ]

Буфер, в котором содержатся данные для записи в удаленный ключ

*question* [in]

Тип: byte [ ]

Указатель на буфер, содержащий расшифрованное 64-битное число-вопрос.

*algNum\_GSII64* [in]

Тип: int

Номер алгоритма типа GSII64, который будет использоваться для шифрования ответа.

*algNum\_HashS3* [in]

Тип: int

Номер алгоритма типа HASH64, который будет использоваться для вычисления хэш-функции для проверки подлинности ответа.

*answer* [out]

byte []

Указатель на буфер, в который будет помещен зашифрованный ответ.

**Возможные ошибки**

|                                          |                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">GrdE.AlgoNotFound</a>        | Аппаратный алгоритм с заданным номером не существует                                      |
| <a href="#">GrdE.CRCErrFunc</a>          | Ошибка при вызове аппаратного алгоритма                                                   |
| <a href="#">GrdE.InactiveItem</a>        | Аппаратный алгоритм деактивирован, обращение к нему невозможно                            |
| <a href="#">GrdE.SystemDataCorrupted</a> | Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует) |
| <a href="#">GrdE.NoQuestion</a>          | Число-вопрос не было сгенерировано или было перегенерировано до записи числа ответа       |
| <a href="#">GrdE.InvalidData</a>         | Неверный формат данных для удаленного программирования                                    |
| <a href="#">GrdE.QuestionOK</a>          | Число-вопрос уже было сгенерировано, ключ ожидает данных для удаленного программирования  |
| <a href="#">GrdE.UpdateNotComplete</a>   | Ошибка при записи данных удаленного программирования. Операция не была завершена          |
| <a href="#">GrdE.InvalidHash</a>         | Неверное значение MAC (Message Authentication Code)                                       |
|                                          | <a href="#">Набор ошибок Guardant API</a>                                                 |

Метод **GrdTRU\_EncryptAnswer** предназначен для подготовки данных (ответа) при использовании технологии Trusted Remote Update.

При подготовке ответа метод **GrdTRU\_EncryptAnswer** генерирует зашифрованный ответ. Этот ответ представляет собой последовательность команд и набор данных. Расшифровка ответа, проверка его подлинности, последующее выполнение команд и запись данных *data* по адресу *addr* производится непосредственно микропрограммой внутри удаленного электронного ключа.

Поскольку кроме данных *data*, которые должны быть записаны в память удаленного ключа, ответ содержит команды и другую служебную информацию, длина ответа *answer* получается больше, чем длина данных. Соответственно для размещения ответа необходимо зарезервировать необходимую память.

Метод проверяет, достаточно ли памяти выделено для ответа, и если размер буфера недостаточен, возвращается код ошибки [GrdE.InvalidArg](#).

Шифрование ответа производится аппаратным алгоритмом типа GSII64 с номером [GrdAN.GSII64](#). На момент шифрования этот алгоритм должен быть создан в ключе, находящемся у разработчика. В качестве определителя должен использоваться секретный 128-битовый ключ, который был сгенерирован и прошит в ключ удаленного пользователя при предпродажной подготовке методом [GrdTRU\\_SetKey](#) для ключа с ID, равным *id*. При использовании GRDUTIL этот ключ берется из базы данных или из соответствующей маски электронного ключа.

Для последующей проверки подлинности ответа производится вычисление хеш-функции аппаратным алгоритмом типа Hash64 с номером задаваемым через параметр [GrdAN.Hash64](#). На момент вычисления этот алгоритм должен быть создан в ключе, находящемся у разработчика. В качестве определителя должен использоваться секретный 128-битовый ключ, который был сгенерирован и прошит в ключ удаленного пользователя при предпродажной подготовке методом [GrdTRU\\_SetKey](#) для ключа с ID равным *id*. При использовании GRDUTIL этот ключ берется из базы данных.

Рабочий ключ, находящийся у разработчика, не обязательно должен быть инициализирован также методом [GrdTRU\\_SetKey](#) с секретным ключом, таким же как у удаленного пользователя. Все преобразования делаются на заранее запрограммированных алгоритмах, номера которых указываются в параметрах указываемых в параметрах [GrdAN.GSII64](#) и [GrdAN.Hash64](#).

**Java**

```
public static GrdE GrdTRU_EncryptAnswer(Handle grdHandle, int addr, byte[] data, byte[] question, int algoNum_GSII64, int algoNum_HashS3, byte[] answer, int[] answerSize)
```

*grdHandle* [in]

Тип: [Handle](#)

Нэндл, через который будет выполнена данная операция.

*addr* [in]

Тип: int

Стартовый адрес (в системе адресации SAM) в памяти удаленного ключа, по которому будет производиться запись данных.

*data* [in]

Тип: byte [ ]

Буфер, в котором содержатся данные для записи в удаленный ключ

*question [in]*

Тип: byte [ ]

Указатель на буфер, содержащий расшифрованное 64-битное число-вопрос.

*algoNum\_GSII64 [in]*

Тип: int

Номер алгоритма типа GSII64, который будет использоваться для шифрования ответа.

*algoNum\_HashS3 [in]*

Тип: int

Номер алгоритма типа HASH64, который будет использоваться для вычисления хэш-функции для проверки подлинности ответа.

*answer [out]*

byte [ ]

Указатель на буфер, в который будет помещен зашифрованный ответ.

*answerSize [in,out]*

int [ ]

Указатель на переменную, которая при вызове должна содержать значение длины буфера *answer*. После вызова в нее будет записан размер буфера *answer*, использованный для размещения ответа.

**Возможные ошибки**

|                                          |                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">GrdE.AlgoNotFound</a>        | Аппаратный алгоритм с заданным номером не существует                                      |
| <a href="#">GrdE.CRCErrFunc</a>          | Ошибка при вызове аппаратного алгоритма                                                   |
| <a href="#">GrdE.InactiveItem</a>        | Аппаратный алгоритм деактивирован, обращение к нему невозможно                            |
| <a href="#">GrdE.SystemDataCorrupted</a> | Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует) |
| <a href="#">GrdE.NoQuestion</a>          | Число-вопрос не было сгенерировано или было регенерировано до записи числа ответа         |
| <a href="#">GrdE.InvalidData</a>         | Неверный формат данных для удаленного программирования                                    |
| <a href="#">GrdE.QuestionOK</a>          | Число-вопрос уже было сгенерировано, ключ ожидает данных для удаленного программирования  |
| <a href="#">GrdE.UpdateNotComplete</a>   | Ошибка при записи данных удаленного программирования. Операция не была завершена          |
| <a href="#">GrdE.InvalidHash</a>         | Неверное значение MAC (Message Authentication Code)                                       |
|                                          | <a href="#">Набор ошибок Guardant API</a>                                                 |

Метод **GrdTRU\_EncryptAnswer** предназначен для подготовки данных (ответа) при использовании технологии Trusted Remote Update.

При подготовке ответа метод **GrdTRU\_EncryptAnswer** генерирует зашифрованный ответ. Этот ответ представляет собой последовательность команд и набор данных. Расшифровка ответа, проверка его подлинности, последующее выполнение команд и запись данных *data* по адресу *addr* производится непосредственно микропрограммой внутри удаленного электронного ключа.

Поскольку кроме данных *data*, которые должны быть записаны в память удаленного ключа, ответ содержит команды и другую служебную информацию, длина ответа *answer* получается больше, чем длина данных. Соответственно для размещения ответа необходимо зарезервировать необходимую память.

Метод проверяет, достаточно ли памяти выделено для ответа, и если размер буфера недостаточен, возвращается код ошибки [GrdE.InvalidArg](#). При этом в переменную *answerSize* записывается минимальный размер буфера для генерации ответа. Это значение необходимо учитывать при повторном выделении памяти для буфера.

Шифрование ответа производится аппаратным алгоритмом типа GSII64 с номером [GrdAN.GSII64](#). На момент шифрования этот алгоритм должен быть создан в ключе, находящемся у разработчика. В качестве определителя должен использоваться секретный 128-битовый ключ, который был сгенерирован и прошит в ключ удаленного пользователя при предпродажной подготовке методом [GrdTRU\\_SetKey](#) для ключа с ID, равным *id*. При использовании GRDUTIL этот ключ берется из базы данных или из соответствующей маски электронного ключа.

Для последующей проверки подлинности ответа производится вычисление хеш-функции аппаратным алгоритмом типа Hash64 с номером задаваемым через параметр [GrdAN.Hash64](#). На момент вычисления этот алгоритм должен быть создан в ключе, находящемся у разработчика. В качестве определителя должен использоваться секретный 128-битовый ключ, который был сгенерирован и прошит в ключ удаленного пользователя при предпродажной подготовке методом [GrdTRU\\_SetKey](#) для ключа с ID равным *id*. При использовании GRDUTIL этот ключ берется из базы данных.

Рабочий ключ, находящийся у разработчика, не обязательно должен быть инициализирован также методом [GrdTRU\\_SetKey](#) с секретным ключом, таким же как у удаленного пользователя. Все преобразования делаются на заранее запрограммированных алгоритмах, номера которых указываются в параметрах указываемых в параметрах [GrdAN.GSII64](#) и [GrdAN.Hash64](#).