GrdTRU_EncryptAnswerEx

Функция(или метод) **GrdTRU_EncryptAnswerEx** предназначены для подготовки данных (ответа) при использовании технологии Trusted Remote Update с возможностью использования новых алгоритмов (AES128 и SHA256). Эту функцию(или метод) необходимо использовать для ключей Guardant Code.

C

```
int GRD_API GrdTRU_EncryptAnswerEx(
  HANDLE hGrd,
  DWORD dwAddr,
  DWORD dwLng,
  void *pData,
  DWORD dwLngQuestion,
  void *pQuestion,
  DWORD dwAlgoNum_Encrypt,
  DWORD dwAlgoNum_Hash,
  void *pAnswer,
  DWORD *pdwAnswerSize,
  DWORD dwMode,
  DWORD dwReserved,
  void *pReserved
);
```

hGrd	хэндл, через который будет выполнена данная операция. В ключ, соответствующий этому хэндлу должен быть записан тот же секретный ключ, что и в удаленном ключе. Также ключ должен содержать алгоритмы GSII64 (AES128) и HASH64 (SHA256), в качестве определителей которых используется секретный ключ
dwAddr	стартовый адрес (в системе адресации SAM) в памяти удаленного ключа, по которому будет производиться запись данных
dwLng	длина буфера данных, которые должны быть записаны в удаленный ключ
pData	буфер, содержащий данные для записи в удаленный ключ
dwLngQuestion	размер присланного удаленным пользователем параметра число-вопрос
pQuestion	указатель на буфер, содержащий расшифрованное число-вопрос
dwAlgoNum_Encrypt	номер алгоритма типа GSII64(AES128), который будет использоваться для зашифрования ответа. Определителем алгоритма должен быть тот же секретный 128-битный ключ, что был записан операцией GrdTRU_SetKey в удаленный ключ
dwAlgoNum_Hash	номер алгоритма типа HASH64(SHA256), 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 GrdTRU_SetKey в удаленный ключ
pAnswer	указатель на буфер, в который будет помещен зашифрованный ответ. Под буфер рекомендуется выделять памяти не менее dwLng*3 + 128 байт
pdwAnswerSize	указатель на переменную типа **DWORD**, которая при вызове должна содержать значение длины буфера *pAnswer*. После вызова в нее будет записан размер буфера *pAnswer*, использованный для размещения ответа. Если изначально размер буфера был меньше необходимого, функция возвращает код ошибки GrdE_InvalidArg. В таком случае это значение необходимо использовать в качестве минимального размера при выделении нового буфера
dwMode	константа определяющая режим работы: GrdTRU_CryptMode_GSII64 — шифрование на базе GSII64 (8 байт), хеш на базе GSII64 (8 байт) GrdTRU_CryptMode_AES128SHA256 — шифрование на базе AES128(16 байт), хеш на базе SHA256(32 байт)
dwReserved	не используется. Параметр должен быть равен 0.
pReserved	не используется. Параметр должен быть равен **NULL**.

Возможные ошибки

GrdE_AlgoNotFound	Аппаратный алгоритм с заданным номером не существует
GrdE_CRCErrorFunc	Ошибка при вызове аппаратного алгоритма
GrdE_InactiveItem	Аппаратный алгоритм деактивирован, обращение к нему невозможно
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_EncryptAnswerEx** предназначена для подготовки данных (ответа) при использовании технологии Trusted Remote Update.

При подготовке ответа функция **GrdTRU_EncryptAnswerEx** 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_Encrypt*. 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_Hash*. 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_Encrypt* и *dwAlgoNum_Hash*.

C#

```
public static GrdE GrdTRU_EncryptAnswerEx(Handle grdHandle, uint addr, byte[] data, byte[] question,
        GrdAlgNum algNumEncrypt,GrdAlgNum algNumHash, out byte[] answer, GrdTRU truMode)
```

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 число-вопрос.

algNumEncrypt [in]

Тип: GrdAlgNum

Номер алгоритма типа GSII64(AES128), который будет использоваться для шифрования ответа.

algNumHash [in]

Тип: GrdAlgNum

Номер алгоритма типа HASH64(SHA256), который будет использоваться для вычисления хэш-функции для проверки подлинности ответа.

answer [out]

byte [ ]

Указатель на буфер, в который будет помещен зашифрованный ответ.

truMode [in]

Тип:GrdTRU

Константа, которая определяет режим работы.
Возможные ошибки

GrdE.AlgoNotFound	Аппаратный алгоритм с заданным номером не существует
GrdE.CRCErrorFunc	Ошибка при вызове аппаратного алгоритма
GrdE.InactiveItem	Аппаратный алгоритм деактивирован, обращение к нему невозможно
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

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

При подготовке ответа метод **GrdTRU_EncryptAnswerEx** 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 памяти больше, чем размер данных.

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.Encrypt. 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.Hash. 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.Encrypt и GrdAN.Hash.

Java

```
public static GrdE GrdTRU_EncryptAnswerEx(Handle grdHandle, int addr, byte[] data, byte[] question, int
algoNum_Encrypt,
        int algoNum_Hash, byte[] answer, int[] answerSize, GrdTRU truMode)
```

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 число-вопрос.

algoNum_Encrypt [in]

Тип: int

Номер алгоритма типа GSII64(AES128), который будет использоваться для шифрования ответа.

algoNum_Hash [in]

Тип: int

Номер алгоритма типа HASH64(SHA256), 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]

Тип: 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.

truMode [in]

Тип:GrdTRU

Константа, которая определяет режим работы.

Возможные ошибки

GrdE.AlgoNotFound	Аппаратный алгоритм с заданным номером не существует
GrdE.CRCErrorFunc	Ошибка при вызове аппаратного алгоритма
GrdE.InactiveItem	Аппаратный алгоритм деактивирован, обращение к нему невозможно

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

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

При подготовке ответа метод **GrdTRU_EncryptAnswerEx** 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 памяти больше, чем размер данных.

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.Encrypt. 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.Hash. 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.Encrypt и GrdAN.Hash.