GrdTRU_DecryptQuestionEx

Функция(метод) **GrdTRU_DecryptQuestionEx** расшифровывает число-вопрос и проверяет подлинность его и остальных присланных с удаленного компьютера параметров с возможностью использования новых алгоритмов **(AES128** и **SHA256).**

C

```
int GRD_API GrdTRU_DecryptQuestionEx(
  HANDLE hGrd,
  DWORD dwAlgoNum_Decrypt,
  DWORD dwAlgoNum_Hash,
  DWORD dwLngQuestion,
  void *pQuestion,
  DWORD dwID,
  DWORD dwPublic,
  DWORD dwLngHash,
  void *pHash,
  DWORD dwMode,
  DWORD dwReserved,
  void *pReserved
);
```

hGrd	хэндл, через который будет выполнена данная операция.
dwAlgoNum_Decrypt	номер аппаратного алгоритма, который будет использоваться для расшифровывания числа-вопроса.
dwAlgoNum_Hash	номер аппаратного алгоритма, который будет использоваться для проверки подлинности числа-вопроса на основании MAC
dwLngQuestion	размер присланного удаленным пользователем параметра число-вопрос
pQuestion	буфер, содержащий присланное удаленным пользователем число-вопрос.
dwID	ID ключа удаленного пользователя, для которого будет произведена операция
dwPublic	численное значение Public Code ключа удаленного пользователя, для которого будет произведена операция
dwLngHash	длина данных в буфере, содержащий MAC, вычисленный на ключе удаленного пользователя.
pHash	буфер, содержащий MAC, вычисленный на ключе удаленного пользователя. Длина буфера 8 байт
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**.
pQuestion	после выполнения функции в этот буфер возвращается расшифрованное число-вопрос.

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

Использование функции **GrdTRU_DecryptQuestionEx** позволяет получить число-вопрос в расшифрованном виде и убедиться в том, что оно действительно было сгенерировано на ключе с ID равным *dwID* и Public Code равным *dwPublic*. Если число-вопрос расшифровано правильно и проверка подлинности прошла успешно, функция возвращает GrdE_OK.

Расшифрованное число-вопрос помещается в тот же буфер *pQuestion*, в котором находилось зашифрованное число-вопрос. Расшифрованное число-вопрос необходимо для генерации ответа, поэтому его нужно сохранить для дальнейшего использования.

Расшифрование числа-вопроса производится аппаратным алгоритмом типа GSII64 (AES128) с номером, задаваемым *dwAlgoNum_Decrypt*. На момент расшифровывания 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.*

Проверка подлинности числа-вопроса производится аппаратным алгоритмом типа Hash64 (SHA256) с номером *dwAlgoNum_Hash*. На момент проверки 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_Decrypt* и *dwAlgoNum_Hash*.

C#

```
public static GrdE GrdTRU_DecryptQuestionEx(Handle grdHandle, GrdAlgNum algNumDecrypt, GrdAlgNum algNumHash,
byte[] question,
        uint id, uint publicCode, byte[] hash, GrdTRU truMode)
```

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

algNumDecrypt [in]

Тип: GrdAlgNum

Номер аппаратного алгоритма, который будет использоваться для расшифровывания числа-вопроса.

algNumHash [in]

Тип: GrdAlgNum

Номер аппаратного алгоритма, который будет использоваться для проверки подлинности числа-вопроса на основании MAC

question [in,out]

Тип: byte [ ]

Буфер, который содержит присланный удаленным пользователем число-вопрос.

id [in]

Тип: uint

ID ключа удаленного пользователя, для которого будет произведена операция.

publicCode [in]

Тип: uint

Численное значение PublicCode ключа удаленного пользователя, для которого будет произведена операция.

hash [in]

Тип: byte [ ]

Буфер, который содержит MAC, вычисленный на ключе удаленного пользователя. Длина буфера 8 байт

truMode [in]

Тип: GrdTRU

Константа, которая определяет режим работы.

question	после выполнения функции в этот буфер возвращается расшифрованное число-вопрос.

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

Использование метода **GrdTRU_DecryptQuestionEx** позволяет получить число-вопрос в расшифрованном виде и убедиться в том, что оно действительно было сгенерировано на ключе с ID равным *id* и Public Code равным *publicCode*. Если число-вопрос расшифровано правильно и проверка подлинности прошла успешно, метод возвращает GrdE.OK.

Расшифрованное число-вопрос помещается в тот же буфер *question*, в котором находилось зашифрованное число-вопрос. Расшифрованное число-вопрос необходимо для генерации ответа, поэтому его нужно сохранить для дальнейшего использования.

Расшифрование числа-вопроса производится аппаратным алгоритмом типа GSII64 (AES128) с номером, задаваемым GrdAN.Decrypt. На момент расшифровывания 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.

Проверка подлинности числа-вопроса производится аппаратным алгоритмом типа Hash64 (SHA256) с номером GrdAN.Hash. На момент проверки 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.Decrypt и GrdAN.Hash.

Java

```
public static GrdE GrdTRU_DecryptQuestionEx(Handle grdHandle, int algoNum_Decrypt, int algoNum_Hash,
        byte[] question, int id, int publicCode, byte[] hash, GrdTRU truMode)
```

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

algNum_Decrypt [in]

Тип: int

Номер аппаратного алгоритма, который будет использоваться для расшифровывания числа-вопроса.

algNum_Hash [in]

Тип: int

Номер аппаратного алгоритма, который будет использоваться для проверки подлинности числа-вопроса на основании MAC

question [in,out]

Тип: byte [ ]

Буфер, который содержит присланный удаленным пользователем число-вопрос.

id [in]

Тип: int

ID ключа удаленного пользователя, для которого будет произведена операция.

publicCode [in]

Тип: int

Численное значение PublicCode ключа удаленного пользователя, для которого будет произведена операция.

hash [in]

Тип: byte [ ]

Буфер, который содержит MAC, вычисленный на ключе удаленного пользователя. Длина буфера 8 байт

truMode [in]

Тип: GrdTRU

Константа, которая определяет режим работы.

question	после выполнения функции в этот буфер возвращается расшифрованное число-вопрос.

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

Использование метода **GrdTRU_DecryptQuestionEx** позволяет получить число-вопрос в расшифрованном виде и убедиться в том, что оно действительно было сгенерировано на ключе с ID равным *id* и Public Code равным *publicCode*. Если число-вопрос расшифровано правильно и проверка подлинности прошла успешно, метод возвращает GrdE.OK.

Расшифрованное число-вопрос помещается в тот же буфер *question*, в котором находилось зашифрованное число-вопрос. Расшифрованное число-вопрос необходимо для генерации ответа, поэтому его нужно сохранить для дальнейшего использования.

Расшифрование числа-вопроса производится аппаратным алгоритмом типа GSII64 (AES128) с номером, задаваемым GrdAN.Decrypt. На момент расшифровывания 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.

Проверка подлинности числа-вопроса производится аппаратным алгоритмом типа Hash64 (SHA256) с номером GrdAN.Hash. На момент проверки 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.Decrypt и GrdAN.Hash.