GrdTRU_DecryptQuestion

Функция(метод) **GrdTRU_DecryptQuestion** расшифровывает число-вопрос и проверяет подлинность его и остальных присланных с удаленного компьютера параметров.

C

```
int GRD_API GrdTRU_DecryptQuestion(
  HANDLE hGrd,
  DWORD dwAlgoNum_GSII64,
  DWORD dwAlgoNum_Hash64,
  void *pQuestion,
  DWORD dwID,
  DWORD dwPublic,
  void *pHash
);
```

hGrd	хэндл, через который будет выполнена данная операция
dwAlgoNum_GSII64	номер аппаратного алгоритма типа GSII64, который будет использоваться для расшифровывания числа-вопроса
dwAlgoNum_Hash64	номер аппаратного алгоритма Hash64, который будет использоваться для проверки подлинности числа-вопроса на основании MAC
pQuestion	буфер, содержащий присланное удаленным пользователем число-вопрос. Длина буфера 8 байт
dwID	ID ключа удаленного пользователя, для которого будет произведена операция
dwPublic	численное значение Public Code ключа удаленного пользователя, для которого будет произведена операция
pHash	буфер, содержащий MAC, вычисленный на ключе удаленного пользователя. Длина буфера 8 байт
pQuestion	после выполнения функции в этот буфер возвращается расшифрованное число-вопрос. Длина буфера 8 байт

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_DecryptQuestion** 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 8-байтовое 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 с номером, задаваемым *dwAlgoNum_GSII64*. 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 с номером *dwAlgoNum_Hash64*. 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 *dwAlgoNum_GSII64* и *dwAlgoNum_Hash64*.

C#

```
public static GrdE GrdTRU_DecryptQuestion(Handle grdHandle, GrdAlgNum algNum_GSII64, GrdAlgNum algNum_HashS3,
byte[] question,
        uint id, uint publicCode, byte[] hash)
```

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

algNum_GSII64 [in]

Тип: GrdAlgNum

Номер аппаратного алгоритма типа GSII64, который будет использоваться для расшифровывания числа-вопроса.

algNum_HashS3 [in]

Тип: GrdAlgNum

Номер аппаратного алгоритма Hash64, 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, содержащий MAC, вычисленный на ключе удаленного пользователя. Длина буфера 8 байт.

question	после выполнения функции в этот буфер возвращается расшифрованное число-вопрос. Длина буфера 8 байт

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_DecryptQuestion** 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 8-байтовое 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 с номером, задаваемым GrdAN.GSII64. 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 с номером GrdAN.Hash64. 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 GrdAN.GSII64 и GrdAN.Hash64.

Java

```
public static GrdE GrdTRU_DecryptQuestion(Handle grdHandle, int algoNum_GSII64, int algoNum_HashS3,
        byte[] question, int id, int publicCode, byte[] hash)
```

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

algNum_GSII64 [in]

Тип: int

Номер аппаратного алгоритма типа GSII64, который будет использоваться для расшифровывания числа-вопроса.

algNum_HashS3 [in]

Тип: int

Номер аппаратного алгоритма Hash64, 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, содержащий MAC, вычисленный на ключе удаленного пользователя. Длина буфера 8 байт.

question	после выполнения функции в этот буфер возвращается расшифрованное число-вопрос. Длина буфера 8 байт

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_DecryptQuestion** 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 8-байтовое 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 с номером, задаваемым GrdAN.GSII64. 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 с номером GrdAN.Hash64. 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 GrdAN.GSII64 и GrdAN.Hash64.