GrdTRU_DecryptQuestionTimeEx

Функция(метод) **GrdTRU_DecryptQuestionTimeEx** расшифровывает число-вопрос и проверяет подлинность его и остальных присланных с удаленного компьютера параметров. Функция(метод) является аналогом GrdTRU_DecryptQuestionEx для ключа Guardant Code Time с возможностью использования новых алгоритмов **(AES128** и **SHA256).**

C

```
int GRD_API GrdTRU_DecryptQuestionTimeEx(
  HANDLE hGrd,
  DWORD dwAlgoNum_Decrypt,
  DWORD dwAlgoNum_Hash,
  DWORD dwLngQuestion,
  void *pQuestion,
  DWORD dwID,
  DWORD dwPublic,
  QWORD *pqwDongleTime,
  QWORD *pqwDeadTimes,
  DWORD dwDeadTimesNumbers,
  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
pqwDongleTime	зашифрованное значение времени ключа. 8 байт.
pqwDeadTimes	зашифрованные значения времён жизни алгоритмов. По 8 байт.
dwDeadTimesNumbers	количество 8 байтовых элементов в *pqwDeadTimes*
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. 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_DecryptQuestionTimeEx** 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*. Функция является аналогом GrdTRU_DecryptQuestionEx для ключа Guardant Time и используется в случаях, когда необходимо продлевать время работы защищенного приложения.

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 (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 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, инициализировать функцией GrdTRU_SetKey с секретным ключом, таким же как у удаленного пользователя, необязательно. Все преобразования делаются на заранее запрограммированных алгоритмах, номера которых указываются в параметрах указываемых в параметрах *dwAlgoNum_Decrypt* и *dwAlgoNum_Hash*.

После расшифрования в *pqwDongleTime* содержится расшифрованное время ключа из микросхемы таймера, а в *pqwDeadTimes* расшифрованное время деактивации алгоритмов.

Два старших байта параметра *pqwDongleTime* - нули. 2 старших байта элементов массива *pqwDeadTimes* - числовое имя алгоритма. Остальные 6 байт - время жизни соответствующего алгоритма.

Время жизни (8 байт) имеет следующий формат:

1, 2 байты	числовое имя алгоритма (либо нули, если время из микросхемы таймера);
3 байт	год от 2000 (08 для 2008 года);
4 байт	месяц года (01 - январь, 02 - февраль, ...);
5 байт	день месяца (1 - 31);
6 байт	часы (0 - 23);
7 байт	минуты (0 - 59);
8 байт	секунды (0 - 59)

C#

```
public static GrdE GrdTRU_DecryptQuestionTimeEx(Handle grdHandle, GrdAlgNum algNumDecrypt, GrdAlgNum
algNumHash, byte[] question,
        uint id, uint publicCode, ref ulong dongleTime, ulong[] deadTimes, int deadTimesNumbers, 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]

Тип: byte [ ]

Буфер, содержащий присланное удаленным пользователем число-вопрос.

id [in]

Тип: uint

ID ключа удаленного пользователя, для которого будет произведена операция.

publicCode [in]

Тип: uint

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

dongleTime [in]

Тип: ulong

Зашифрованное значение времени ключа.

deadTimes [in]

Тип: ulong [ ]

Зашифрованные значения времён жизни алгоритмов.

deadTimesNumbers [in]

Тип: int

Количество 8 байтовых элементов в DeadTimes.

hash [in]

Тип: byte [ ]

Буфер, содержащий MAC, вычисленный на ключе удаленного пользователя.

truMode [in]

Тип: GrdTRU

Константа определяющая режим работы.

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 метода **GrdTRU_DecryptQuestionTimeEx** 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*. Метод является аналогом GrdTRU_DecryptQuestionEx для ключа Guardant Time и используется в случаях, когда необходимо продлевать время работы защищенного приложения.

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.

Расшифровка числа-вопроса производится аппаратным алгоритмом типа GSII64 (AES128) с номером, задаваемым GrdAN.Decrypt. На момент расшифровки 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, инициализировать методом GrdTRU_SetKey с секретным ключом, таким же как у удаленного пользователя, необязательно. Все преобразования делаются на заранее запрограммированных алгоритмах, номера которых указываются в параметрах указываемых в параметрах GrdAN.Decrypt и GrdAN.Hash64.

После расшифровки в *dongleTime* содержится расшифрованное время ключа из микросхемы таймера, а в *DeadTimes* расшифрованное время деактивации алгоритмов.

Два старших байта параметра *dongleTime* - нули. 2 старших байта элементов массива *deadTimes* - числовое имя алгоритма. Остальные 6 байт - время жизни соответствующего алгоритма.

Время жизни (8 байт) имеет следующий формат:

1, 2 байты	числовое имя алгоритма (либо нули, если время из микросхемы таймера);
3 байт	год от 2000 (08 для 2008 года);
4 байт	месяц года (01 - январь, 02 - февраль, ...);
5 байт	день месяца (1 - 31);
6 байт	часы (0 - 23);
7 байт	минуты (0 - 59);
8 байт	секунды (0 - 59)

Java

```
public static GrdE GrdTRU_DecryptQuestionTimeEx(Handle grdHandle, int algoNum_Decrypt, int algoNum_Hash,
        byte[] question, int id, int publicCode, long[] dongleTime, long[] deadTimes, int deadTimesNumbers, byte
[] hash, int mode)
```

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

algoNum_Decrypt [in]

Тип: int

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

algoNum_Hash [in]

Тип: int

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

question [in]

Тип: byte [ ]

Буфер, содержащий присланное удаленным пользователем число-вопрос.

id [in]

Тип: int

ID ключа удаленного пользователя, для которого будет произведена операция.

publicCode [in]

Тип: int

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

dongleTime [in]

Тип: long [ ]

Зашифрованное значение времени ключа.

deadTimes [in]

Тип: long [ ]

Зашифрованные значения времён жизни алгоритмов.

deadTimesNumbers [in]

Тип: int

Количество 8 байтовых элементов в DeadTimes.

hash [in]

Тип: byte [ ]

Буфер, содержащий MAC, вычисленный на ключе удаленного пользователя.

mode [in]

Тип: int

Константа определяющая режим работы.

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 метода **GrdTRU_DecryptQuestionTimeEx** 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*. Метод является аналогом GrdTRU_DecryptQuestionEx для ключа Guardant Time и используется в случаях, когда необходимо продлевать время работы защищенного приложения.

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.

Расшифровка числа-вопроса производится аппаратным алгоритмом типа GSII64 (AES128) с номером, задаваемым GrdAN.Decrypt. На момент расшифровки 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, инициализировать методом GrdTRU_SetKey с секретным ключом, таким же как у удаленного пользователя, необязательно. Все преобразования делаются на заранее запрограммированных алгоритмах, номера которых указываются в параметрах указываемых в параметрах GrdAN.Decrypt и GrdAN.Hash64.

После расшифровки в *dongleTime* содержится расшифрованное время ключа из микросхемы таймера, а в *DeadTimes* расшифрованное время деактивации алгоритмов.

Два старших байта параметра *dongleTime* - нули. 2 старших байта элементов массива *deadTimes* - числовое имя алгоритма. Остальные 6 байт - время жизни соответствующего алгоритма.

Время жизни (8 байт) имеет следующий формат:

1, 2 байты	числовое имя алгоритма (либо нули, если время из микросхемы таймера);
3 байт	год от 2000 (08 для 2008 года);
4 байт	месяц года (01 - январь, 02 - февраль, ...);
5 байт	день месяца (1 - 31);
6 байт	часы (0 - 23);
7 байт	минуты (0 - 59);
8 байт	секунды (0 - 59)