GrdTRU_GenerateQuestionTimeEx

Функция(метод) **GrdTRU_GenerateQuestionTimeEx** генерирует зашифрованное число-вопрос для удаленного программирования, использующего технологию Trusted Remote Update. Является аналогом функции(метода) GrdTRU_GenerateQuestionEx для ключа Guardant Code Time с возможностью использования новых алгоритмов **(AES128** и **SHA256).**

C

```
int GRD_API GrdTRU_GenerateQuestionTimeEx(
  HANDLE hGrd,
  DWORD dwLngQuestion,
  void *pQuestion,
  DWORD *pdwID,
  DWORD *pdwPublic,
  QWORD *pqwDongleTime,
  DWORD dwDeadTimesSize,
  QWORD *pqwDeadTimes,
  DWORD *pdwDeadTimesNumbers,
  DWORD dwLngHash,
  void *pHash,
  DWORD dwReserved,
  void *pReserved
);
```

hGrd	хэндл, через который будет выполнена данная операция
dwLngQuestion	размер буфера, куда будет помещен сгенерированный вопрос.
pQuestion	буфер, куда будет помещен сгенерированный вопрос.
pdwID	буфер, куда будет помещено значение ID ключа, для которого сгенерирован вопрос.
pdwPublic	буфер, куда будет помещено численное значение Public code ключа, для которого сгенерирован вопрос.
pqwDongleTime	зашифрованное время из микросхемы таймера. Длина буфера 8 байт
dwDeadTimesSize	размер входного буфера *pqwDeadTimes* в байтах
pqwDeadTimes	зашифрованные значения времен жизни алгоритмов. По 8 байт
pdwDeadTimesNumbers	количество элементов, возвращаемых в *pqwDeadTimes*
dwLngHash	размер буфера , куда будет помещено значение MAC (Message Authentication Code - кода аутентификации сообщения) для верификации вопроса.
pHash	буфер, куда будет помещено значение MAC (Message Authentication Code - кода аутентификации сообщения) для верификации вопроса.
dwReserved	зарезервировано. Должно быть равно 0
pReserved	зарезервировано. Должно быть равно **NULL**

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

Функция **GrdTRU_GenerateQuestionTimeEx** генерирует зашифрованное число-вопрос и инициализирует процесс для удаленного программирования, использующего технологию Trusted Remote Update. Функция является аналогом GrdTRU_GenerateQuestionEx для ключа Guardant Time и используется в случаях, когда необходимо продлевать время работы защищенного приложения.

Функция **GrdTRU_GenerateQuestionTimeEx** вызывается на компьютере удаленного пользователя и генерирует число-вопрос *pQuestion*, защищенное от подделки кодом аутентификации сообщения (MAC) *pHash*. MAC вырабатывается аппаратным алгоритмом на секретном ключе, который должен быть предварительно записан при помощи функции GrdTRU_SetKey. MAC используется для того, чтобы нельзя было подделать число-вопрос, ID или Public Code электронного ключа.

После того, как число-вопрос сгенерировано, конечный пользователь должен передать разработчику все сгенерированные функцией **GrdTRU_GenerateQuestionTimeEx** данные: собственно число-вопрос *pQuestion*, ID ключа *pdwID*, Public code *pdwPublic* и MAC *pHash*. С момента генерации числа-вопроса ключ переходит в состояние ожидания числа-ответа.

Рекомендуемый размер буфера *pqwDeadTimes* для зашифрованного значения времени жизни алгоритмов должен быть равен (количеству алгоритмов + количество защищенных ячеек)*8. Если буфер содержит меньше элементов, то возвращается только то, что поместилось, иначе дополняется нулями до *dwDeadTimesSize*/8 элементов, но не более 499 элементов.

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)

На клиентской стороне всегда можно узнать, сколько алгоритмов и ячеек есть в ключе для вычисления количества элементов массива **DeadTime**. Количество алгоритмов и защищенных ячеек в ключе можно узнать, считав поле **kmAlgoNum** в режиме адресации SAM.

На стороне разработчика тоже можно вычислить количество алгоритмов по маске, хранящейся в базе. Поэтому в функциях TRU для Time важен только размер массива. Более того, количество элементов можно передать в "посылке" удаленного программирования вместе с числом-вопросом.

C#

```
public static GrdE GrdTRU_GenerateQuestionTimeEx(Handle grdHandle, out byte[] question, out uint id, out uint
publicCode,
        out ulong dongleTime, ulong[] deadTimes, out int deadTimesNumbers, out byte[] hash)
```

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

question [out]

Тип: byte [ ]

Буфер, куда будет помещен сгенерированный вопрос.

id [out]

Тип: uint

Буфер, куда будет помещено значение ID ключа, для которого был сгенерирован вопрос.

publicCode [out]

Тип: uint

Буфер, куда будет помещено значение PublicCode ключа, для которого был сгенерирован вопрос.

dongleTime [out]

Тип: ulong

Зашифрованное время из микросхемы таймера.

deadTimes [out]

Тип: ulong [ ]

Зашифрованное значение времен жизни алгоритмов.

deadTimesNumbers [out]

Тип: int

Количество элементов, возвращаемых в deadTimes.

hash [out]

Тип: byte [ ]

Буфер, куда будет помещено значение MAC (Message Authentication Code - кода аутентификации сообщения) для верификации вопроса.
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

Метод **GrdTRU_GenerateQuestionTimeEx** генерирует зашифрованное число-вопрос и инициализирует процесс для удаленного программирования, использующего технологию Trusted Remote Update. Метод является аналогом GrdTRU_GenerateQuestionEx для ключа Guardant Time и используется в случаях, когда необходимо продлевать время работы защищенного приложения.

Метод **GrdTRU_GenerateQuestionTimeEx** вызывается на компьютере удаленного пользователя и генерирует число-вопрос *question*, защищенное от подделки кодом аутентификации сообщения (MAC) *hash*. MAC вырабатывается аппаратным алгоритмом на секретном ключе, который должен быть предварительно записан при помощи метода GrdTRU_SetKey. MAC используется для того, чтобы нельзя было подделать число-вопрос, ID или Public Code электронного ключа.

После того, как число-вопрос сгенерировано, конечный пользователь должен передать разработчику все сгенерированные методом **GrdTRU_GenerateQuestionTimeEx** данные: собственно число-вопрос *question*, ID ключа *id*, Public code *publicCode* и MAC *hash*. С момента генерации числа-вопроса ключ переходит в состояние ожидания числа-ответа.

Рекомендуемый размер буфера *deadTimes* для зашифрованных значения времени жизни алгоритмов должен быть равен (количеству алгоритмов + количество защищенных ячеек)*8. Если буфер содержит меньше элементов, то возвращается только то, что поместилось, иначе дополняется нулями до *deadTimesNumbers*/8 элементов, но не более 499 элементов.

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)

На клиентской стороне всегда можно узнать, сколько алгоритмов и ячеек есть в ключе для вычисления количества элементов массива *deadTime*. Количество алгоритмов и защищенных ячеек в ключе можно узнать, считав поле **kmAlgoNum** в режиме адресации SAM.

На стороне разработчика тоже можно вычислить количество алгоритмов по маске, хранящейся в базе. Поэтому в функциях TRU для Time важен только размер массива. Более того, количество элементов можно передать в "посылке" удаленного программирования вместе с числом-вопросом.

Java

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

grdHandle [in]

Тип: Handle

Нэндл, через который будет выполнена данная операция.

question [out]

Тип: byte [ ]

Буфер, куда будет помещен сгенерированный вопрос.

id [out]

Тип: int [ ]

Буфер, куда будет помещено значение ID ключа, для которого был сгенерирован вопрос.

publicCode [out]

Тип: int [ ]

Буфер, куда будет помещено значение PublicCode ключа, для которого был сгенерирован вопрос.

dongleTime [out]

Тип: long [ ]

Зашифрованное время из микросхемы таймера.

deadTimes [out]

Тип: long [ ]

Зашифрованное значение времен жизни алгоритмов.

deadTimesNumbers [out]

Тип: long [ ]

Количество элементов, возвращаемых в deadTimes.

hash [out]

Тип: byte [ ]

Буфер, куда будет помещено значение MAC (Message Authentication Code - кода аутентификации сообщения) для верификации вопроса.
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

Метод **GrdTRU_GenerateQuestionTimeEx** генерирует зашифрованное число-вопрос и инициализирует процесс для удаленного программирования, использующего технологию Trusted Remote Update. Метод является аналогом GrdTRU_GenerateQuestionEx для ключа Guardant Time и используется в случаях, когда необходимо продлевать время работы защищенного приложения.

Метод **GrdTRU_GenerateQuestionTimeEx** вызывается на компьютере удаленного пользователя и генерирует число-вопрос *question*, защищенное от подделки кодом аутентификации сообщения (MAC) *hash*. MAC вырабатывается аппаратным алгоритмом на секретном ключе, который должен быть предварительно записан при помощи метода GrdTRU_SetKey. MAC используется для того, чтобы нельзя было подделать число-вопрос, ID или Public Code электронного ключа.

После того, как число-вопрос сгенерировано, конечный пользователь должен передать разработчику все сгенерированные методом **GrdTRU_GenerateQuestionTimeEx** данные: собственно число-вопрос *question*, ID ключа *id*, Public code *publicCode* и MAC *hash*. С момента генерации числа-вопроса ключ переходит в состояние ожидания числа-ответа.

Рекомендуемый размер буфера *deadTimes* для зашифрованных значения времени жизни алгоритмов должен быть равен (количеству алгоритмов + количество защищенных ячеек)*8. Если буфер содержит меньше элементов, то возвращается только то, что поместилось, иначе дополняется нулями до *deadTimesNumbers*/8 элементов, но не более 499 элементов.

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)

На клиентской стороне всегда можно узнать, сколько алгоритмов и ячеек есть в ключе для вычисления количества элементов массива *deadTime*. Количество алгоритмов и защищенных ячеек в ключе можно узнать, считав поле **kmAlgoNum** в режиме адресации SAM.

На стороне разработчика тоже можно вычислить количество алгоритмов по маске, хранящейся в базе. Поэтому в функциях TRU для Time важен только размер массива. Более того, количество элементов можно передать в "посылке" удаленного программирования вместе с числом-вопросом.