

GrdTRU_GenerateQuestionEx

Функция(метод) **GrdTRU_GenerateQuestionEx** генерирует зашифрованное число-вопрос для удаленного программирования, использующего технологию Trusted Remote Update с возможностью использования новых алгоритмов (AES128 и SHA256). Эту функцию(метод) необходимо использовать для ключей Guardant Code.

C

```
int GRD_API GrdTRU_GenerateQuestionEx(
    HANDLE hGrd,
    DWORD dwLngQuestion,
    void *pQuestion,
    DWORD *pdwID,
    DWORD *pdwPublic,
    DWORD dwLngHash,
    void *pHash,
    DWORD dwReserved,
    void *pReserved
);
```

<i>hGrd</i>	хэндл, через который будет выполнена данная операция
<i>dwLngQuestion</i>	размер буферу, куда будет помещен сгенерированный вопрос.
<i>pQuestion</i>	буфер, куда будет помещен сгенерированный вопрос.
<i>pdwID</i>	буфер, куда будет помещено значение ID ключа, для которого сгенерирован вопрос.
<i>pdwPublic</i>	буфер, куда будет помещено численное значение Public code ключа, для которого сгенерирован вопрос.
<i>dwLngHash</i>	размер буфера, куда будет помещено значение MAC (Message Authentication Code - кода аутентификации сообщения) для верификации вопроса.
<i>pHash</i>	буфер, куда будет помещено значение MAC (Message Authentication Code - кода аутентификации сообщения) для верификации вопроса.
<i>dwReserved</i>	зарезервировано, должно быть равно 0
<i>pReserved</i>	зарезервировано, должно быть равно NULL
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_GenerateQuestionEx** генерирует зашифрованное число-вопрос и инициализирует процесс для удаленного программирования, использующего технологию Trusted Remote Update.

Функция **GrdTRU_GenerateQuestionEx** 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_GenerateQuestionEx** 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.

C#

```
public static GrdE GrdTRU_GenerateQuestionEx(Handle grdHandle, out byte[] question, out uint id, out uint publicCode, 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 численное значение PublicCode ключа, для которого был сгенерирован вопрос.

hash [out]

Тип: byte []

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

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_GenerateQuestionEx** генерирует зашифрованное число-вопрос и инициализирует процесс для удаленного программирования, использующего технологию Trusted Remote Update.

Метод **GrdTRU_GenerateQuestionEx** 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_GenerateQuestionEx** 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.

Java

```
public static GrdE GrdTRU_GenerateQuestionEx(Handle grdHandle, byte[] question, int[] id, byte[] publicCode, 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: byte []

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

hash [out]

Тип: byte []

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

GrdE.SystemDataCorrupted	Системные данные TRU повреждены. (Секретный ключ удаленного программирования отсутствует)	
GrdE.NoQuestion	Число-вопрос не было сгенерировано или было регенерировано 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_GenerateQuestionEx** генерирует зашифрованное число-вопрос и инициализирует процесс для удаленного программирования, использующего технологию Trusted Remote Update.

Метод **GrdTRU_GenerateQuestionEx** 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_GenerateQuestionEx** 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.