GrdSign

Функция(метод) **GrdSign** вычисляет электронно-цифровую подпись входного сообщения при помощи аппаратно-реализованного криптографического алгоритма ECC160.

Синтаксис

C

```
int GRD_API GrdSign(
  HANDLE hGrd,
  DWORD        dwAlgoNum,
  DWORD        dwDataLng,
  void *pData,
  DWORD        dwSignResultLng,
  void *pSignResult,
  void *pReserved
);
```

hGrd [in]	хэндл, через который будет выполнена данная операция
dwAlgoNum [in]	номер дескриптора алгоритма электронно-цифровой подписи ECC160
dwDataLng [in]	длина входного сообщения (20 байт для ECC160)
pData [in]	указатель на входное сообщение
dwSignResultLng [in]	длина выходного буфера для электронно-цифровой подписи (40 байт для ECC160)
pSignResult [out]	указатель на выходной буфер, в который будет сохранена электронно-цифровая подпись
pReserved	зарезервировано

GrdE_OK	нет ошибок
GrdE_InvalidArg	недопустимый параметр при вызове функции
GrdE_NoService	для алгоритма/ячейки сервис не предусмотрен
GrdE_AlgoNotFound	алгоритма с указанным числовым именем не существует
GrdE_GPis0	счетчик алгоритма достиг нулевого значения

Функция **GrdSign** позволяет вычислить электронно-цифровую подпись (ЭЦП) входного сообщения с помощью аппаратного алгоритма ЭЦП. Микропрограмма внутри электронного ключа считывает дескриптор алгоритма с заданным числовым именем, проверяет отсутствие в нём блокировок и только после этого переходит к выполнению операции.

Дескриптор алгоритма с заданным в параметре *dwAlgoNum* номером должен присутствовать в памяти ключа, в противном случае функция возвращает ошибку GrdE_AlgoNotFound. Если в дескрипторе алгоритма установлен флаг "уменьшение счетчика", то вычитание счетчика алгоритма происходит при каждом вызове **GrdSign**. При достижении счетчиком нулевого значения, возвращается ошибка GrdE_GPis0. Если при создании алгоритма или в процессе работы он был переведен в неактивное состояние, возвращается ошибка GrdE_InactiveItem. При попытке вызвать функцию для моделей ключей Stealth II или Stealth III, возвращается ошибка GrdE_NoService.

Длина входного сообщения задаётся параметром *dwDataLng*. Сообщение для подписи должно находиться по адресу, указанному в параметре *pData*. Буфер для ЭЦП должен быть зарезервирован заранее, а его длина передана функции через параметр *dwSignResultLng*. Функция проверяет входные указатели и длины на нулевые значение и возвращает GrdE_InvalidArg, если любое из значений окажется нулевым. В случае успешного выполнения, по адресу *pSignResult* будет находится вычисленная ЭЦП от входного сообщения, при этом функция возвращает GrdE_OK. Для алгоритма ECC160 длина входного сообщения и длина возвращаемой электронно-цифровой подписи должны быть **GrdECC160_MESSAGE_SIZE** и **GrdECC160_DIGEST_SIZE** соответственно.

C#

```
public static GrdE GrdSign(Handle grdHandle, GrdAlgNum algNum, byte[] data, out byte[] digestSign)
```

grdHandle [in]

Тип: Handle

Хэндл, через который будет выполнена данная операция.

algNum [in]

Тип: GrdAlgNum

Номер дескриптора алгоритма электронно-цифровой подписи ECC160.

data [in]

Тип: byte [ ]

Входное сообщение для подписи.

digestSign [out]

Тип: byte [ ]

Выходной буфер, в который будет сохранена электронно-цифровая подпись.

GrdE.OK	нет ошибок
GrdE.InvalidArg	недопустимый параметр при вызове функции
GrdE.NoService	ключ не поддерживает данную функцию
GrdE.AlgoNotFound	алгоритма с указанным числовым именем не существует
GrdE.GPis0	счетчик алгоритма достиг нулевого значения

Метод **GrdSign** позволяет вычислить электронно-цифровую подпись (ЭЦП) входного сообщения с помощью аппаратного алгоритма ЭЦП. Микропрограмма внутри электронного ключа считывает дескриптор алгоритма с заданным числовым именем, проверяет отсутствие в нём блокировок и только после этого переходит к выполнению операции.

Дескриптор алгоритма с заданным в параметре *dwAlgoNum* номером должен присутствовать в памяти ключа, в противном случае метод возвращает ошибку GrdE.AlgoNotFound. Если в дескрипторе алгоритма установлен флаг "уменьшение счетчика", то вычитание счетчика алгоритма происходит при каждом вызове **GrdSign**. При достижении счетчиком нулевого значения, возвращается ошибка GrdE.GPis0. Если при создании алгоритма или в процессе работы он был переведен в неактивное состояние, возвращается ошибка GrdE.InactiveItem. При попытке вызвать метод для моделей ключей Stealth II или Stealth III, возвращается ошибка GrdE.NoService.

Сообщение для подписи должно находиться в массиве *data*. Буфер для ЭЦП должен быть зарезервирован заранее и передан методу через параметр *digestSign.* Если длина любого из массивов окажется нулевой, метод возвращает GrdE.InvalidArg. В случае успешного выполнения, в массиве *digestSign* будет находится вычисленная ЭЦП от входного сообщения, при этом метод возвращает GrdE.OK. Для алгоритма ECC160 длина входного сообщения и длина возвращаемой электронно-цифровой подписи должны быть GrdECC160.MESSAGE_SIZE и GrdECC160.DIGEST_SIZE соответственно.

Java

```
public static GrdE GrdSign(Handle grdHandle, int algNum, byte[] data, byte[] sign)
```

grdHandle [in]

Тип: Handle

хэндл, через который будет выполнена данная операция.

algNum [in]

Тип: int

Номер дескриптора алгоритма электронно-цифровой подписи ECC160.

data [in]

Тип: byte [ ]

Входное сообщение для подписи.

sign [out]

Тип: byte [ ]

Выходной буфер, в который будет сохранена электронно-цифровая подпись.

GrdE.OK	нет ошибок
GrdE.InvalidArg	недопустимый параметр при вызове функции
GrdE.NoService	ключ не поддерживает данную функцию
GrdE.AlgoNotFound	алгоритма с указанным числовым именем не существует
GrdE.GPis0	счетчик алгоритма достиг нулевого значения

Метод **GrdSign** позволяет вычислить электронно-цифровую подпись (ЭЦП) входного сообщения с помощью аппаратного алгоритма ЭЦП. Микропрограмма внутри электронного ключа считывает дескриптор алгоритма с заданным числовым именем, проверяет отсутствие в нём блокировок и только после этого переходит к выполнению операции.

Дескриптор алгоритма с заданным в параметре *dwAlgoNum* номером должен присутствовать в памяти ключа, в противном случае метод возвращает ошибку GrdE.AlgoNotFound. Если в дескрипторе алгоритма установлен флаг "уменьшение счетчика", то вычитание счетчика алгоритма происходит при каждом вызове **GrdSign**. При достижении счетчиком нулевого значения, возвращается ошибка GrdE.GPis0. Если при создании алгоритма или в процессе работы он был переведен в неактивное состояние, возвращается ошибка GrdE.InactiveItem. При попытке вызвать метод для моделей ключей Stealth II или Stealth III, возвращается ошибка GrdE.NoService.

Сообщение для подписи должно находиться в массиве *data*. Буфер для ЭЦП должен быть зарезервирован заранее и передан методу через параметр s*ign.* Если длина любого из массивов окажется нулевой, метод возвращает GrdE.InvalidArg. В случае успешного выполнения, в массиве s*ign* будет находится вычисленная ЭЦП от входного сообщения, при этом метод возвращает GrdE.OK. Для алгоритма ECC160 длина входного сообщения и длина возвращаемой электронно-цифровой подписи должны быть GrdECC160.MESSAGE_SIZE и GrdECC160.DIGEST_SIZE соответственно.