

GccaSign

Функция **GccaSign** вычисляет электронную цифровую подпись блока байт при помощи аппаратного алгоритма **ECC160**.

С

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

<i>hGrd</i>	не используется
<i>dwAlgoNum</i>	числовое имя аппаратного алгоритма типа ECC Algorithm
<i>dwDataLng</i>	длина массива данных (20 байтов для ECC160)
<i>pData</i>	указатель на массив данных
<i>dwSignResultLng</i>	длина массива цифровой подписи (40 байтов для ECC160)
<i>pSignResult</i>	указатель на массив цифровой подписи
<i>pPrivateKey</i>	указатель на буфер с секретным (закрытым) ключом
<i>pReserved</i>	зарезервировано

GrdE_OK	нет ошибок
GrdE_NeedInitialization	требуется инициализация API (вызов GrdStartup)
GrdE_InvalidHandle	недействительный хэндл
GrdE_InvalidArg	недопустимый параметр при вызове функции
GrdE_NoService	ключ не поддерживает данную функцию
GrdE_AlgoNotFound	алгоритма с указанным числовым именем не существует
GrdE_CRCErrorFunc	ошибка CRC при выполнении функции
GrdE_GPis0ошибка	счетчик алгоритма достиг нулевого значения

Функция **GccaSign** позволяет вычислять цифровую подпись массива данных при помощи аппаратного алгоритма типа ECC. Вычисление цифровой подписи производится алгоритмом с числовым именем, заданным в параметре *dwAlgoNum*. Этот алгоритм предварительно должен быть создан.

Если в дескрипторе алгоритма установлен флаг **nsafl_GP_dec** (уменьшение счетчика), вычитание счетчика GP происходит при каждом вызове **GccaSign**.

Длина массива данных (в байтах) *pData* задается параметром *dwDataLng* и зависит от типа алгоритма.

Длина возвращаемой цифровой подписи (в байтах) *pSignResult* также зависит от типа алгоритма и задаётся параметром *dwSignResultLng*.

Для алгоритма **ECC160** длина массива данных и длина возвращаемой цифровой подписи должны быть **GrdECC160_MESSAGE_SIZE** (20 байт) и **GrdECC160_DIGEST_SIZE** (40 байт) соответственно. Может работать как через защищенные ячейки типа алгоритм, так и напрямую обращаться к алгоритму **ECC160** (GrdSS_ECC160 в параметре *dwAlgo*).