GccaVerifySign

Функция **GccaVerifySign** проверяет электронную цифровую подпись блока байт при помощи аппаратного алгоритма ECC160.

C

```
int GccaVerifySign(
  HANDLE hGrd,
  DWORD dwAlgoType,
  DWORD dwPublicKeyLng,
  void *pPublicKey,
  DWORD dwDataLng,
  void *pData,
  DWORD dwSignLng,
  void *pSign,
  void *pReserved
);
```

hGrd	не используется
dwAlgoType	тип программного алгоритма (см. **GrdVSC_XXXXX)**
dwPublicKeyLng	длина открытого ключа
pPublicKey	указатель на открытый ключ
dwDataLng	длина массива данных (20 байтов для **ECC160)**
pData	указатель на массив данных
dwSignLng	длина массива цифровой подписи (40 байтов для **ECC160)**
pSign	указатель на массив цифровой подписи
pReserved	зарезервировано

GrdE_OK	нет ошибок
GrdE_NeedInitialization	требуется инициализация API (вызов GrdStartup)
GrdE_InvalidHandle	недействительный хэндл
GrdE_InvalidArg	недопустимый параметр при вызове функции
GrdE_InvalidPublicKey	недействительный открытый ключ
GrdE_InvalidDigitalSign	недействительная цифровая подпись

Функция **GccaVerifySign** осуществляет проверку цифровой подписи массива данных. Реализация функции полностью программная. Проверка цифровой подписи производится алгоритмом, заданным в параметре *dwAlgoType*. Типы допустимых программных алгоритмов определены константами **GrdVSC_XXXXX**. Длина открытого ключа (в байтах) *pPublicKey* задаётся параметром *dwPublicKeyLng* и зависит от типа программного алгоритма. Длины массива данных (в байтах) *pData* и цифровой подписи (в байтах) *pSign* задаются параметрами *dwDataLng* и *dwSi gnLng* соответственно.

Для алгоритма **ECC160** тип программного алгоритма должен быть **GrdVSC_ECC160**.

Длина открытого ключа должна быть **GrdECC160_PUBLIC_KEY_SIZE** (40 байт). Длина массива данных и длина цифровой подписи должны быть **GrdECC160_MESSAGE_SIZE** (20 байт) и **GrdECC160_DIGEST_SIZE** (40 байт) соответственно.