GrdVerifySign

Функция(метод) **GrdVerifySign** проверяет электронную цифровую подпись блока данных при помощи программного алгоритма.

C

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

hGrd	хэндл, через который будет выполнена данная операция
dwAlgoType	тип программного алгоритма (см. **GrdVSC_ECC160)**
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 **GrdVerifySign** осуществляет проверку цифровой подписи массива данных. Реализация функции полностью программная.

Проверка цифровой подписи производится алгоритмом, заданным в параметре *dwAlgoType*.

Типы допустимых программных алгоритмов определены единственной константой **GrdVSC_ECC160**. Она определяет алгоритм ECC160

Длина открытого ключа (в байтах) pPublicKey задаётся параметром *dwPublicKeyLng* и зависит от возможного типа программного алгоритма.

Длины массива данных (в байтах) pData и цифровой подписи (в байтах) *pSign* задаются параметрами *dwDataLng* и *dwSignLng* соответственно.

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.

C#

```
public static GrdE GrdVerifySign(Handle grdHandle, byte[] publicKey, byte[] data, byte[] digestSign)
```

grdHandle [in]

Тип: Handle

хэндл, через который будет выполнена данная операция.

publicKey [in]

Тип: byte [ ]

Длина открытого ключа.

data [in]

Тип: byte [ ]

Указатель на массив данных.

digestSign [in]

Тип: byte [ ]

Указатель на массив цифровой подписи.

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

Метод **GrdVerifySign** осуществляет проверку цифровой подписи массива данных. Реализация метода полностью программная.

Типы допустимых программных алгоритмов определены единственной константой GrdVSC.ECC160. Она определяет алгоритм ECC160.

Длина открытого ключа (в байтах) *publicKey* зависит от возможного типа программного алгоритма.

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.

Java

```
public static GrdE GrdVerifySign(Handle grdHandle, byte[] publicKey, byte[] data, byte[] sign)
```

grdHandle [in]

Тип: Handle

хэндл, через который будет выполнена данная операция.

publicKey [in]

Тип: byte [ ]

Длина открытого ключа.

data [in]

Тип: byte [ ]

Указатель на массив данных.

sign [in]

Тип: byte [ ]

Указатель на массив цифровой подписи.

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

Метод **GrdVerifySign** осуществляет проверку цифровой подписи массива данных. Реализация метода полностью программная.

Типы допустимых программных алгоритмов определены единственной константой GrdVSC.ECC160. Она определяет алгоритм ECC160.

Длина открытого ключа (в байтах) *publicKey* зависит от возможного типа программного алгоритма.

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.