GrdVerifyDigest

Описание

Проверяет цифровую подпись данных при помощи криптографического алгоритма ECC160.

Сначала функция автоматически вычисляет ХЕШ от проверяемых данных на алгоритме SHA-256, после чего выполняется проверка подписи полученной ХЕШ-суммы.

Синтаксис

```
int GRD_API GrdVerifyDigest(grd_uint32 publicKeySize,
                                                    const void* publicKey,
                                                    grd_uint32 messageSize,
                                                    const void* message,
                                                    grd_uint32 digestSize,
                                                    const void* digest);
```

Параметры

`publicKeySize`	Размер (в байтах) открытого ключа. Допустимое значение: 40 байт
`publicKey`	Указатель на буфер с открытым ключом. У каждого компонента (Feature) свой открытый ключ. Он указан в интерфейсе Guardant Station в разделе Компоненты на странице конкретного компонента
`messageSize`	Размер (в байтах) буфера с данными подпись которых необходимо проверить. Допустимое значение: 20 байт
`message`	Указатель на буфер с данными подпись которых необходимо проверить
`digestSize`	Размер (в байтах) буфера цифровой подписи. Допустимое значение: 40 байт
`digest`	Указатель на буфер проверяемой цифровой подписи

Возвращаемые значения

GRD_OK

GRD_INVALID_FEATURE