GccaHash

Функция **GccaHash** вычисляет хэш-функцию блока данных.

C

```
int GccaHash(
  HANDLE hGrd,
  DWORD dwHash,
  DWORD dwDataLng,
  void *pData,
  DWORD dwMethod,
  void *pDigest,
  void *pKeyBuf,
  void *pContext
);
```

hGrd	не используется
dwHash	поддерживает только алгоритм типа **SHA256** GrdSH_SHA256 — Алгоритм SHA256
dwDataLng	длина блока данных, хэш которых будет вычисляться, в байтах.
pData	указатель на буфер данных , хэш которых будет вычисляться
dwMethod	метод преобразования, который задается комбинацией флагов **GrdSC_XXX** GrdSC_First — Первый блок данных GrdSC_Next — Следующий блок данных GrdSC_Last — Последний блок данных GrdSC_All — Единственный блок данных. Хэш считается за один раз
pDigest	Указатель на буфер, куда будет помещен результат вычислений. Для этого буфера должна быть зарезервирована память не менее: • для алгоритма **SHA256** - **GrdSHA256_DIGEST_SIZE**
pKeyBuf	зарезервировано. Параметр должен быть равен **NULL**
pContext	Буфер, длиной **GrdSHA256_CONTEXT_SIZE** для хранения контекста (состояния алгоритма) при последовательном вычислении хэш-функции **SHA256** от нескольких блоков данных. GrdSHA256_DIGEST_SIZE — Размер дайджеста, возвращаемого алгоритмом **SHA256** GrdSHA256_CONTEXT_SIZE — Размер контекста алгоритма **SHA256** для запоминания предыдущего состояния алгоритма

Набор ошибок Guardant API

Функция **GccaHash** вычисляет хэш-функцию блока данных *pData* длиной *dwDataLng*.

В Guardant GccAPI реализовано **SHA256**. Выбор алгоритма осуществляется параметром *dwHash*, который **в настоящий момент равен GrdSH_SHA256**.

Все хэш-функции могут вычисляться от больших блоков данных, поэтому предусмотрена возможность разбиения данных на меньшие блоки и вычисления значения хэша последовательно для нескольких буферов. Для этого параметром *dwMethod* задается порядок блока **GrdSC_XXX** (первый, следующий, последний).

Для передачи состояния алгоритма **SHA256** используется специальный контекст *pContext*, память для которого должна быть зарезервирована и проинициализирована заранее. Функция **GccaHash** самостоятельно разбивает буфер на блоки необходимой длины и выполняет все операции по согласованию.

Если операция выполняется за один прием, то параметром *dwMethod* должен быть задан метод **GrdSC_All**.

Результат вычислений помещается в буфер *pDigest*, память для которого размером, соответствующим конкретному алгоритму, должна быть зарезервирована заранее.

Поддерживает только алгоритм типа **SHA256 (GrdSH_SHA256** в параметре *dwHash*).