



---

# КАРМА

---

Расширение «Поддержка Штампов  
времени»

---

©Электронные Офисные Системы. 2019 г.

---

<b>1. Введение .....</b>	<b>3</b>
<b>2. Интерфейс пользователя .....</b>	<b>3</b>
<b>3. Интерфейс разработчика .....</b>	<b>5</b>
<b>3.1 InitExtensionDll .....</b>	<b>5</b>
<b>3.2 AcquireCryptMsgUnauthAttributes .....</b>	<b>7</b>
<b>3.3. CheckCryptMsgAttributes.....</b>	<b>7</b>
<b>3.4 CheckCryptMsgAttrByOID .....</b>	<b>7</b>
<b>3.5 EnumAttrOIDs .....</b>	<b>7</b>
<b>3.6 Формат словаря ExtensionInfo .....</b>	<b>7</b>
<b>Приложение 1. Список кодов ошибок библиотеки.....</b>	<b>9</b>

## 1. Введение

Службы штампов времени позволяют защищенным образом отслеживать время создания и модификации данных, предоставляя возможность убедиться в том, что данные были созданы до определенного момента времени и не были изменены впоследствии.

Библиотека реализует поддержку клиентской части служб штампов времени описанных в открытом стандарте RFC 3161 и расширяет возможности системы «КАРМА», позволяя встраивать в ЭЦП штамп времени в качестве неаутентифицируемого атрибута.

В рамках спецификации RFC 3161 определены следующие термины:

- Штамп времени (time-stamp) - это подписанное крипто-сообщение, содержащее хэш данных, время выдачи и некоторые другие расширенные параметры штампа.
- Служба штампов времени (Time Stamping Authority - TSA) - доверенный элемент PKI, имеющий доступ к точному источнику времени и оказывающий услуги по созданию штампов времени. Выдавая штамп времени, служба штампов времени удостоверяет, что в момент выдачи ей было предоставлено значение хэша от некоторых данных.

При встраивании штампа времени в ЭЦП, службе штампов времени передается значение хэша подписываемых данных, тем самым позволяя надежно зафиксировать время создания ЭЦП, а впоследствии убедиться, что данная подпись была создана в период действия ее сертификата.

Доступ к TSA производится по протоколу HTTP, с использованием библиотеки WinHTTP входящей в состав ОС Windows.

## 2. Интерфейс пользователя

Интерфейс пользователя библиотеки представляет собой диалоговое окно с информацией о штампе времени, которое изображено на рис.1.

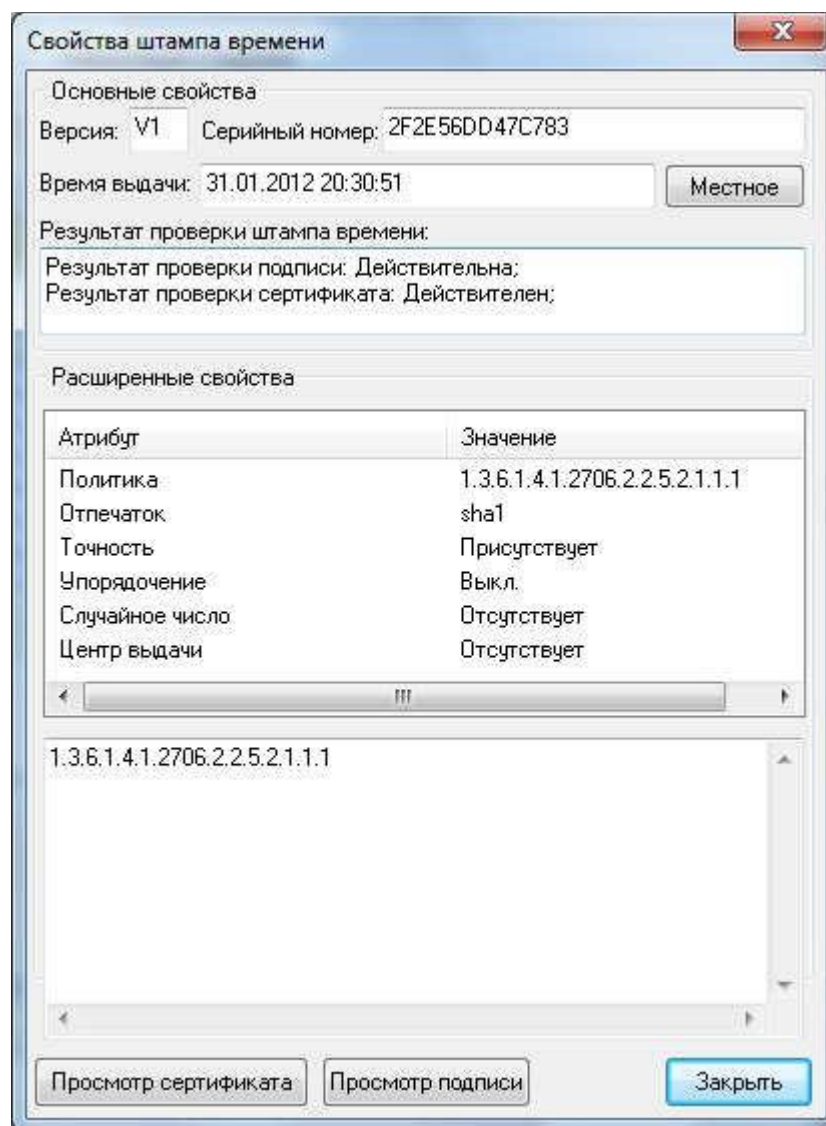


Рис. 1.

Текстовые поля «Версия», «Серийный номер» и «Время выдачи» содержат значения соответствующих параметров штампа времени.

Кнопка с надписью «Местное» позволяет выбрать часовой пояс для отображения времени выдачи штампа (в настоящее время поддерживается переключение между часовым поясом учетной записи пользователя и UTC).

Текстовое поле «Результат проверки штампа времени» содержит информацию о результате проверки подписи и сертификата штампа времени.

Кнопка «Просмотр подписи» предназначена для отображения стандартного диалога Windows с информацией о подписанном крипто-сообщении, которым по сути является штамп времени.

Кнопка «Просмотр сертификата» отображает стандартный диалог ОС Windows с информацией о сертификате службы выдавшей данный штамп времени.

Список «Расширенные свойства» содержит информацию о дополнительных опциях

штампа времени, их наличии или отсутствии. Текстовое окно, расположенное ниже списка предназначено для отображения расширенной информации о выбранном свойстве.

В текущей версии библиотеки поддерживается отображение информации о следующих свойствах:

- Политика – OID политики выдачи данного штампа времени;
- Отпечаток – алгоритм и значение хэш-функции переданной службе штампов времени, для получения данного штампа.
- Точность – оценка погрешности часов службы штампов времени в секундах. Если точность присутствует в данном штампе, то она учитывается при проверке его корректности.
- Упорядочение – параметр, определяющий возможность определить порядок выдачи штампов времени данной службой, пользуясь исключительно временем выдачи.
- Случайное число – случайное число входящее в запрос и ответ службы штампов времени, используется для предотвращения replay-атак.
- Центр выдачи – если свойство присутствует в штампе времени, то содержит полное наименование службы, выдавшей штамп.

### 3. Интерфейс разработчика

Интерфейс разработчика библиотеки соответствует «Спецификации интерфейса модуля добавления и проверки произвольного параметра ЭЦП», регламентирующей набор и порядок применения экспортируемых библиотекой функций.

Данный параграф содержит дополнительные сведения о работе функций интерфейса. Описание кодов ошибок, устанавливаемых библиотекой при помощи функции SetLastError находится в приложении 1.

#### 3.1 InitExtensionDll

Функция получает в качестве параметра текстовую строку, состоящую из именованных свойств и их значений, позволяющих регулировать поведение библиотеки расширения. Синтаксис строки инициализации:

```
parameter1="value1"; parameter2=value2
```

где parameterN – имя свойства, а valueN – его значение,

свойства отделяются символом точки с запятой «;», имя свойства отделяется от значения знаком равенства «=». Если значение свойства является текстовой строкой, то оно должно

быть заключено в двойные кавычки «"». Символы пробела окружающие свойства, значения или символы разделителя не учитываются при анализе строки. Регистр символов имени свойства не учитывается.

При наличии синтаксических ошибок в строке инициализации функция возвращает `FALSE` и библиотека не считается инициализированной. Свойства и значения, не поддерживаемые библиотекой расширения игнорируются.

В настоящее время поддерживаются следующие свойства:

**`TSP_URL="http://path.to.timestamp.service"`**

Значением свойства является URL службы штампов времени.

**`TSP_USE_NONCE="TRUE"`**

Включает использование случайного числа (т.н. nonce) при запросе штампа времени. Служит для предотвращения возможности replay-атак. По умолчанию выключено.

**`TSP_DEFAULT_ACCURACY=9600`**

Значение точности используемое для проверки времени ответа сервера, если в самом ответе точность отсутствует. Указывается в миллисекундах. Значение по умолчанию – 3000 мс. Максимально значение точности – 7200000 (2 часа).

**`TSP_IGNORE_SERVER_ACCURACY="TRUE"`**

Отключает использование точности ответа сервера при проверке времени ответа. Вместо точности сервера используется точность по умолчанию, регулируемая параметром `TSP_DEFAULT_ACCURACY`.

**`TSP_INET_TIMEOUT = 10000`**

Определяет максимальный таймаут для получения ответа сервера в миллисекундах. Если параметр равен 0, то значение таймаута устанавливается равным бесконечности. Если параметр имеет отрицательное значение, то используется значение таймаутов по умолчанию: время разрешения адреса – бесконечность, время соединения – 60с, время отправки запроса – 30с, время приема ответа – 30с.

**`TSP_HASH_ALG_OID="gost-r-34.11-94"`**

Позволяет указать OID алгоритма хеш-функции, применяемой для вычисления дайджеста сообщения, используемого для запроса штампа времени. Помимо непосредственного указания OID параметр поддерживает следующие короткие имена алгоритмов: "md2", "md4", "md5", "sha-1", "sha-256", "sha-384", "sha-512", "gost-r-34.11-94".

По умолчанию используется алгоритм хэширования сертификата подписания.

Для использования расширения в прикладном коде необходимо указать параметры в строке инициализации крипто – интерфейса EOSCrypto.ICrypto. Обязательным является параметр **TSP\_URL**.

### 3.2 AcquireCryptMsgUnauthAttributes

Функция формирует запрос штампа времени, на основе переданных данных (значении хэша подписи) и настроек библиотеки. Отправка запроса службе штампов времени и получение ответа происходят согласно протоколу HTTP с использованием библиотеки WinHTTP.

При отсутствии URL в строке инициализации функция возвращает FALSE и устанавливает значение `LastError` в `ERROR_WINHTTP_INVALID_URL`.

### 3.3. CheckCryptMsgAttributes

Функция проверяет все подписи криптографического сообщения и соподписи первого уровня каждой подписи.

При обнаружении неверных атрибутов штампа времени подписи функция возвращает FALSE, `GetLastError` возвратит соответствующий код ошибки.

При отсутствии атрибутов штампа времени во всех проверяемых подписях и соподписях функция возвращает FALSE, `GetLastError` возвратит `ERROR_NO_DATA`.

### 3.4 CheckCryptMsgAttrByOID

Производит проверку штампа времени и возвращает результат и его описание.

Если параметр `dwCallingFunctionId` равен `mode_getsigninfo`, то в качестве результата возвращается текстовая UNICODE строка с информацией о штампе времени. Описание ключей и значений приведено в п 3.6. В противном случае в качестве значения результата возвращается закодированная структура `TimeStampToken`.

В качестве имени расширения фозвращается текстовая строка «Штамп времени»

### 3.5 EnumAttrOIDs

В данной версии библиотека расширения поддерживает только OID `id-aa-timeStampToken` - 1.2.840.113549.1.9.16.2.14.

### 3.6 Формат словаря ExtensionInfo

`ExtensionInfo` представляет собой словарь `IDictionary` со следующим набором пар ключзначение:

ExtensionName – имя расширения – «Штамп времени»;

ExtensionOID – OID расширения - «1.2.840.113549.1.9.16.2.14»;

ExtensionInterpretedString – строка, содержащая текстовое описание результата проверки – «Штамп времени верен» в случае корректности атрибута;

ExtensionInterpretedData – данные атрибута – в данном случае текстовая строка из пар ключзначение (закодированная в Base64).

Строка состоит из пар ключ – значение разделенных точкой с запятой, ключ отделяется от значения символом знака равенства. В табл.1 приведено описание ключей и соответствующих им значений.

Таблица 1

Ключ	Значение
Version	Версия
Serial	Серийный номер
UtcTime	Время выдачи по Гринвичу
LocalTime	Местное время выдачи
Policy	Политика
HashAlg	Алгоритм хеша
HashValue	Значение хеша
Accuracy	Точность
Ordering	Упорядочение
Nonce	Случайное число
Tsa	Имя службы штампов времени



## Приложение 1. Список кодов ошибок библиотеки

`#define USER_ERR_UNKNOWN` ((DWORD) 0xE0640001L)

Неизвестная ошибка

`#define USER_ERR_WRONG_CMDLINE` ((DWORD) 0xE0640002L)

Неверные параметры командной строки

`#define USER_ERR_NO_INPUT_DATA` ((DWORD) 0xE0640003L)

Отсутствуют входные данные

`#define USER_ERR_BAD_INPUT_DATA` ((DWORD) 0xE0640004L)

Неверные входные данные

`#define USER_ERR_BAD_INIT_STRING` ((DWORD) 0xE0640005L)

Синтаксическая ошибка в строке инициализации

`#define CRYPT_ERR_UNKNOWN` ((DWORD) 0xE0650001L)

Неизвестная ошибка криптографии

`#define CRYPT_ERR_WRONG_STRUCT` ((DWORD) 0xE0650002L)

Неверная структура ASN.1

`#define CRYPT_ERR_SIGN_CERT_ABSENT` ((DWORD) 0xE0650003L)

Отсутствует сертификат подписавшей стороны

`#define CRYPT_ERR_NO_ISSUER_CERT` ((DWORD) 0xE0650004L)

Отсутствует сертификат издателя

`#define CRYPT_ERR_CERT_IS_NOT_TIME_VALID ((DWORD) 0xE0650005L)` Временной  
интервал сертификата неверен

`#define CRYPT_ERR_CHAIN_NOT_VALID ((DWORD) 0xE0650006L)`  
Неверная цепочка сертификатов

`#define CRYPT_ERR_TST_INVALID_RESPONCE ((DWORD) 0xE0650401L)`  
Неверный ответ на запрос штампа времени

`#define CRYPT_ERR_TST_WRONG_SIGN_COUNT ((DWORD) 0xE0650402L)`  
Неверное число подписей штампа времени

`#define CRYPT_ERR_TST_CERT_CHAIN_NOT_VALID ((DWORD) 0xE0650403L)`  
Неверная цепочка сертификатов штампа времени

`#define CRYPT_ERR_TST_CERT_REVOKED ((DWORD) 0xE0650404L)`  
Сертификат штампа времени отозван

`#define CRYPT_ERR_TST_RESP_TIME_NOT_IN_ACCURACY ((DWORD) 0xE0650405L)`  
Время штампа времени не соответствует точности

`#define CRYPT_ERR_TST_POLICY_MISMATCH ((DWORD) 0xE0650406L)`  
Политика штампа времени не соответствует запросу

`#define CRYPT_ERR_TST_NONCE_MISMATCH ((DWORD) 0xE0650407L)`  
Случайное число штампа времени не соответствует запросу

`#define CRYPT_ERR_TST_UNSUPPORTED_REQ_VERSION ((DWORD) 0xE0650408L)`  
Неподдерживаемая версия запроса штампа времени

```
#define CRYPT_ERR_TST_UNSUPPORTED_RESP_VERSION ((DWORD) 0xE0650409L)
```

Неподдерживаемая версия ответа штампа времени

```
#define CRYPT_ERR_TST_REQ_RESP_HASH_MISMATCH ((DWORD) 0xE065040AL)  Хэши запроса  
и ответа штампа времени не совпадают
```

```
#define CRYPT_ERR_TST_MSG_HASH_MISMATCH ((DWORD) 0xE065040BL)
```

Хэши подписи и штампа времени не совпадают

```
#define CRYPT_ERR_TST_WRONG_TST_CONTENTS ((DWORD) 0xE065040CL)
```

Неверное содержимое штампа времени

```
#define CRYPT_ERR_TST_ATTRIBUTE_ABSENT ((DWORD) 0xE065040DL)
```

Отсутствует атрибут штампа времени

```
#define CRYPT_ERR_TST_INVALID_KEY_USAGE ((DWORD) 0xE065040EL)
```

Неверное значение расширенного использования ключа сертификата штампа времени

```
#define CRYPT_ERR_TST_WRONG_ESSCERT ((DWORD) 0xE065040FL)  Атрибут
```

EssCertId подписи штампа времени отсутствует или неверен

```
#define TST_GENERIC_ERROR ((DWORD) 0xE0650410L)
```

```
#define CRYPT_MSG_TST_INVALID_RESPONSE ((DWORD) 0xE0650411L)
```

```
#define CRYPT_ERR_TST_CERT_REVOCATION_UNKNOWN ((DWORD) 0xE0650412L)
```

```
#define INET_ERR_UNKNOWN ((DWORD) 0xE0660001L)
```

Неизвестная ошибка сети

```
#define INET_ERR_RESPONSE_TOO_LARGE ((DWORD) 0xE0660002L)
```

Слишком большая длина ответа

```
#define INET_ERR_BAD_CONTENT_LENGTH ((DWORD) 0xE0660003L) Неверное
```

значение заголовка content length