Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»

Инструкция по применению «Litoria CryptoService»

Листов 16

Санкт-Петербург
2017

АННОТАЦИЯ

В настоящем документе приводится инструкция по применению приложения «Litoria CryptoService» (в дальнейшем по тексту «Litoria CryptoService» или приложение).

В разделе «Назначение» приводятся сведения о функциях «Litoria CryptoService».

В разделе «Установка «Litoria CryptoService» описаны действия, которые необходимо выполнить для установки «Litoria CryptoService» на рабочий компьютер.

В разделе «Использование «Litoria CryptoService» указаны действия, которые необходимо выполнить для осуществления той или иной операции.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ «LITORIA CRYPTOSERVICE»

Основная функция «Litoria CryptoService» - предоставление пользователю доступа к базовым функциям криптографической библиотеки BHGiSCryptography через REST интерфейс.

Приложение «Litoria CryptoService» позволяет:

- обращаться к сертификатам в хранилище сертификатов;
- подписывать информационное сообщение с использованием сертификата электронной подписи (ЭП);
- проверять электронную подпись для информационного сообщения;
- шифровать/расшифровывать информационные сообщения;
- отправлять DVCS-запросы.

2. УСТАНОВКА «LITORIA CRYPTOSERVICE»

Для установки приложения «Litoria CryptoService» запустите файл-инсталлятор «BhCryptoService.msi».

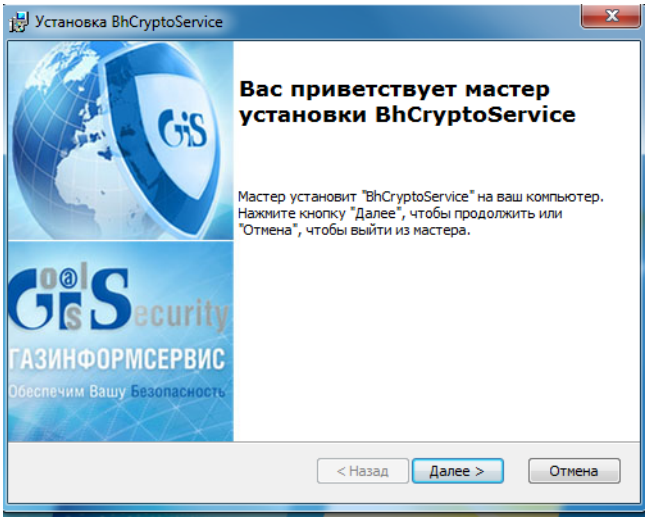


Рисунок 2.1. Окно установки приложения

Нажмите на кнопку *«Далее»*.

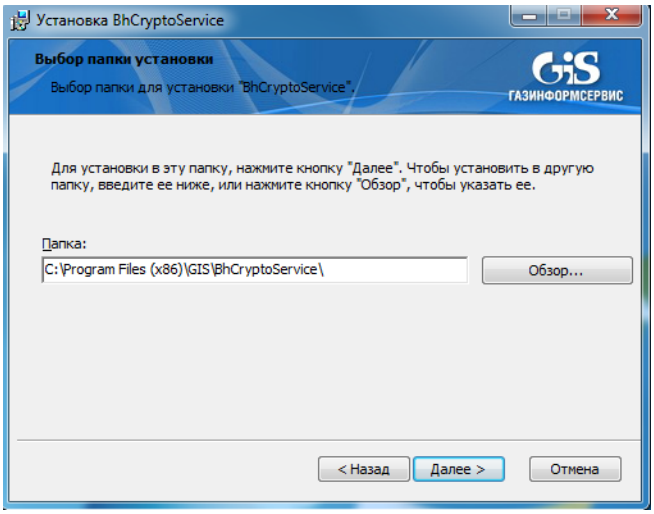


Рисунок 2.2. Выбор папки установки

В появившемся окне (Рисунок 2.2) укажите папку установки приложения. Затем нажмите на кнопку *«Далее»*.

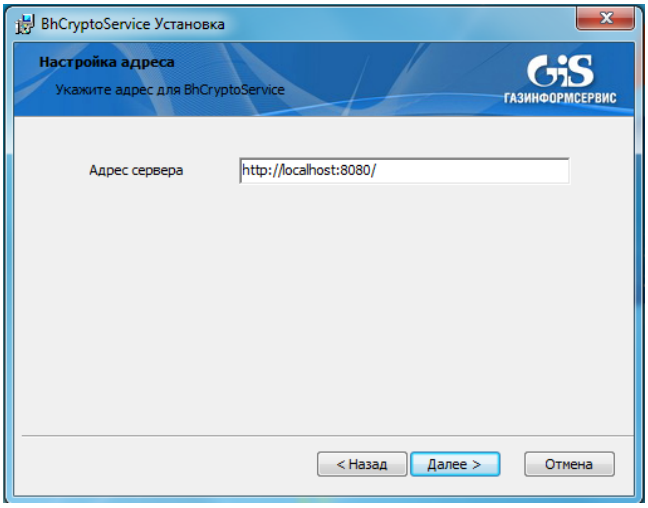


Рисунок 2.3. Настойка адреса для приложения

В появившемся окне (Рисунок 2.3.) задайте адрес веб-службы принимающей REST запросы и порт, на котором запускается служба (по умолчанию установлен порт 8080). Затем нажмите на кнопку *«Далее»*.

Адрес веб-службы и порт, на котором запускается служба, после установки приложения можно изменить в файле «bhcryptoservice.ini», находящемся в папке C:\Users\[Имя пользователя]\AppData\Roaming.

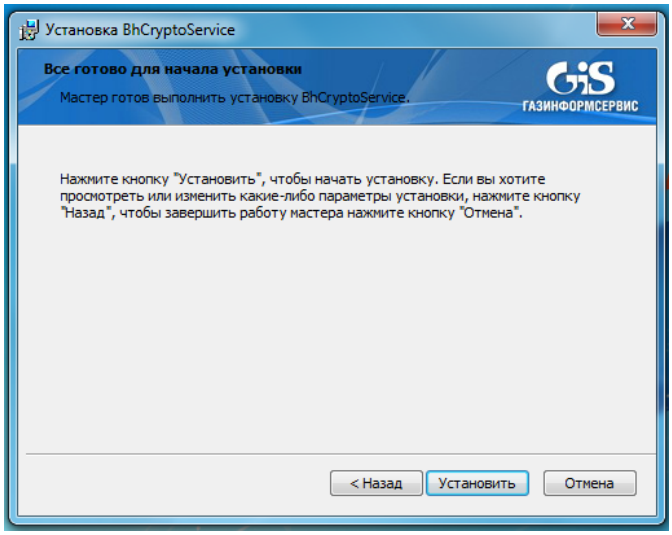


Рисунок 2.4. Начало установки приложения

В появившемся окне (Рисунок 2.4) нажмите на кнопку *«Установить»*.

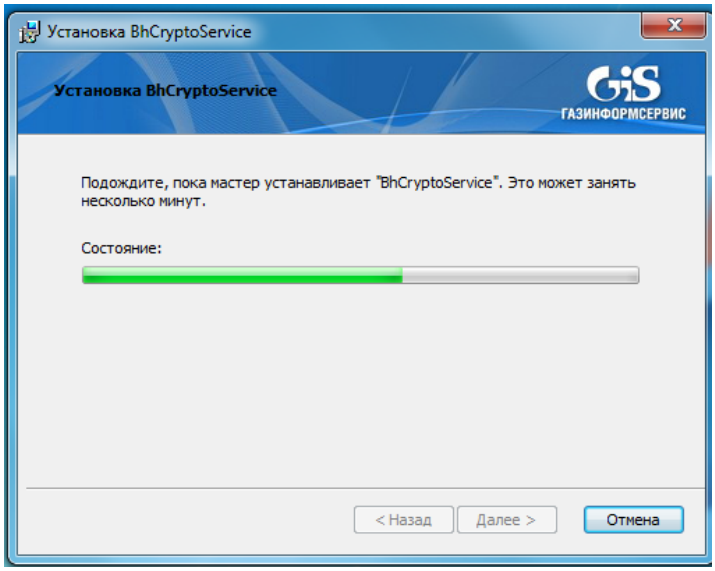


Рисунок 2.5. Процесс установки приложения «Litoria CryptoService»

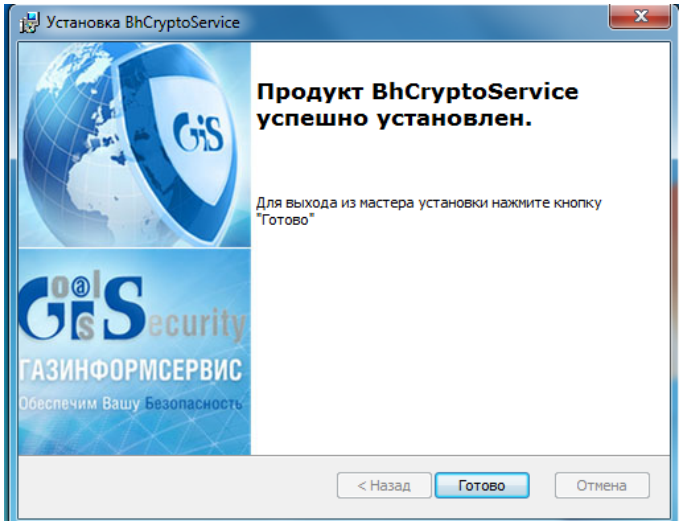


Рисунок 2.6. Завершение установки

Нажмите на кнопку *«Готово»* в окне завершения установки и перезагрузите компьютер.

3. ИСПОЛЬЗОВАНИЕ «LITORIA CRYPTOSERVICE»

3.1. НАЧАЛО РАБОТЫ

Для начала работы с «Litoria CryptoService» необходимо запустить файл «BHCryptoService.exe». Показателем успешного запуска приложения, является значок  на панели задач.

Приложение «Litoria CryptoService» обращается к базовым функциям криптографической библиотеки BHGiSCryptography через REST интерфейс. После установки приложения запускается локальная веб-служба принимающая REST запросы в соответствии с представленным ниже интерфейсом.

Для выполнения функций приложения можно использовать любой REST клиент, например «Advanced REST client» для Google Chrome (Рисунок 3.1).

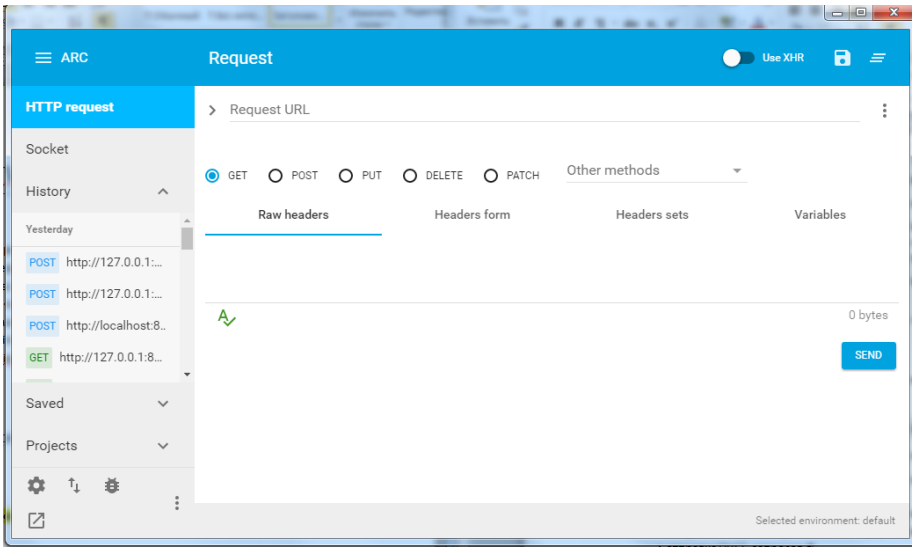


Рисунок 3.1. Главное окно «Advanced REST client»

3.2. ОПИСАНИЕ ФУНКЦИЙ REST ИНТЕРФЕЙСА «LITORIA CRYPTOSERVICE»

Приложение «Litoria CryptoService» позволяет выполнить следующие операции:

- обращение к сертификатам в хранилище сертификатов;
- подпись информационных сообщений с использованием сертификата электронной подписи (ЭП);
- проверка электронной подписи информационных сообщений;
- шифрование/расшифровывание информационных сообщений;
- отправка DVCS-запросов.

3.2.1. ОБРАЩЕНИЕ К ХРАНИЛИЩУ СЕРТИФИКАТОВ

3.2.1.1. ПОЛУЧЕНИЕ ВСЕХ СЕРТИФИКАТОВ ИЗ ХРАНИЛИЩА

Для задания сведений о сертификатах, которые будут использоваться при выполнении команд шифрования или подписи данных, необходимо найти все сертификаты в хранилище сертификатов. Для поиска используется функция «certs», имеющая следующий синтаксис:

http://localhost:8080/certs?Storename=<имя хранилища сертификатов>

Входным параметром для данной функции является:

«Storename»	Имя хранилища сертификатов

Возвращаемые значения - массив структур «CertInfos»:

«CertBody»	Сертификат (BASE64)
«Email»	Почта владельца сертификата
«GivenName»	Имя владельца сертификата
«Id»	Id владельца сертификата
«Inn»	ИНН владельца сертификата
«IssuerInfo»	Сведения о издателе сертификата(BASE64)
«Kpp»	КПП владельца сертификата
«Locality»	Населенный пункт владельца сертификата
«Ogrn»	ОГРН владельца сертификата
«OrgUnit»	Подразделение организации владельца сертификата
«Organization»	Организация владельца сертификата
«SerialNumber»	Серийный номер сертификата (BASE64)
«Snils»	СНИЛС владельца сертификата
«State»	Область владельца сертификата
«StreetAddress»	Адрес владельца сертификата
«SubjectInfoCn»	Общее имя владельца сертификата
«SureName»	Фамилия владельца сертификата
«TimeNotAfter»	Дата истечения сертификата
«TimeNotBefore»	Дата начала действия сертификата
«Title»	Должность владельца сертификата
«UnstructuredName»	Неструктурированное имя владельца сертификата
«isQualified»	Квалифицированность сертификата

Пример: **http://localhost:8080/certs?Storename=MY**

Примеры выполнения функций REST интерфейса «Litoria CryptoService» с использованием «Advanced REST client» представлены в Приложении 1.

3.2.1.2. ПОЛУЧЕНИЕ ОПРЕДЕЛЕННОГО СЕРТИФИКАТА ИЗ ХРАНИЛИЩА

Для нахождения и получения сведений об определенном сертификате в хранилище сертификатов, используется функция «certdata», имеющая следующий синтаксис:

http://localhost:8080/certdata?Storename=<имя хранилища сертификатов>&SerialNumber=<серийный номер сертификата>&IssueInfo=<информация об издателе (BASE64)>

Входными параметрами для данной функции являются:

«Storename»	Имя хранилища сертификатов
«SerialNumber»	Серийный номер (BASE64)
«IssuerInfo»	Информация о издателе (BASE64)

Возвращаемые значения – данные сертификата:

«CertBody»	Сертификат (BASE64)
«Email»	Почта владельца сертификата
«GivenName»	Имя владельца сертификата
«Id»	Id владельца сертификата
«Inn»	ИНН владельца сертификата
«IssuerInfo»	Сведения о издателе сертификата(BASE64)
«Kpp»	КПП владельца сертификата
«Locality»	Населенный пункт владельца сертификата
«Ogrn»	ОГРН владельца сертификата
«OrgUnit»	Подразделение организации владельца сертификата
«Organization»	Организация владельца сертификата
«SerialNumber»	Серийный номер сертификата (BASE64)
«Snils»	СНИЛС владельца сертификата
«State»	Область владельца сертификата
«StreetAddress»	Адрес владельца сертификата
«SubjectInfoCn»	Общее имя владельца сертификата
«SureName»	Фамилия владельца сертификата
«TimeNotAfter»	Дата истечения сертификата
«TimeNotBefore»	Дата начала действия сертификата
«Title»	Должность владельца сертификата
«UnstructuredName»	Неструктурированное имя владельца сертификата
«isQualified»	Квалифицированность сертификата

3.2.1.3. ДОБАВЛЕНИЕ СЕРТИФИКАТА В ХРАНИЛИЩЕ

Для добавления сертификата в хранилище сертификатов, используется функция «installcertdata», имеющая следующий синтаксис:

http://localhost:8080/installcertdata

{
"Storename":"<Имя хранилища сертификатов>",
"Certificate": "<Сертификат (BASE64)>"
}

Входными параметрами для данной функции являются:

«Storename»	Имя хранилища сертификатов
«Certificate»	Сертификат (BASE64)

3.2.1.4. УДАЛЕНИЕ СЕРТИФИКАТА ИЗ ХРАНИЛИЩА

Для удаления сертификата из хранилища сертификатов, используется функция «deletecertdata», имеющая следующий синтаксис:

http://localhost:8080/deletecertdata

{
"Storename":"<Имя хранилища сертификатов>",
"Certificate": "<Сертификат (BASE64)>"
}

Входными параметрами для данной функции являются:

«Storename»	Имя хранилища сертификатов
«Certificate»	Сертификат (BASE64)

3.2.2. СОЗДАНИЕ ЭП ИНФОРМАЦИОННОГО СООБЩЕНИЯ

Для подписания информационного сообщения с использованием сертификата электронной подписи (ЭП) используется функция «sign», имеющая следующий синтаксис:

http://localhost:8080/sign

{
"Data":"< Подписываемая информация в BASE64>",
"Certificate":"< Сертификат (BASE64)>,
"Comment":"< Комментарий к ЭП >",
"PinCode":"< Пинкод сертификата>",
"TspAddress":"< URL сервиса штампа времени >",
"DetachedEDS":< Отделенная подпись (true/false)>,
"AdvancedEDS":< Усовершенствованная подпись (true/false)>,
"IncludeTimeStamp":< Включение штамп времени (true/false)>
}

Входными параметрами для данной функции являются:

«Data»	Подписываемая информация, закодированная в BASE64
«Certificate»	Сертификат (BASE64)

«Comment»	Комментарий к ЭП
«Pincode»	Пинкод сертификата
«TspAddress»	URL сервиса штампа времени(Обязательное значение при флагах AdvancedEDS или IncludeTimeStamp)
«DetachedEDS»	Отделенная ли подпись (True/false)
«AdvancedEDS»	Усовершенствованная ли подпись (True/false)
«IncludeTimeStamp»	Включить ли штамп времени (True/false)

Возвращаемое значение:

«SignData»	Электронная подпись документа (BASE64)

3.2.3. ПРОВЕРКА ЭП ИНФОРМАЦИОННОГО СООБЩЕНИЯ

Для проверки подписи информационного сообщения используется функция «verify», имеющая следующий синтаксис:

http://localhost:8080/verify

{
"SignData":"<Электронная подпись документа (BASE64)>"
}

Входными параметрами для данной функции являются:

«SignData»	Электронная подпись документа (BASE64)

Возвращаемое значение - массив структур «SignInfos»:

Структура «SignInfos»:	
«CertEncoded»	Сертификат (BASE64)
«IsAdvanced»	Усовершенствованная ли подпись (True/False)
«IsCounterSignature»	Заверяющая ли подпись (True/False)
«IsTimestampIncluded»	(True/False)
«SignatureIndex»	Порядковый номер подписи
«SignatureTime»	Время подписи (Структура SignatureTime)
«SignatureValue»	Значение подписи (BASE64)
«VerifyCertificateResult»	Результат проверки действительности сертификата(True/False)
«VerifyResult»	Результат проверки подписи(True/False)

Структура «SignatureTime»	
«wDay»	День (Числовое значение)
«wDayOfWeek»	День недели (Числовое значение)
«wHour»	Час (Числовое значение)
«wMilliseconds»	Миллисекунда (Числовое значение)

«wMinute»	Минута (Числовое значение)
«wMonth»	Месяц (Числовое значение)
«wSecond»	Секунда (Числовое значение)
«wYear»	Год (Числовое значение)

Для проверки отделенной подписи информационного сообщения функция «verify», имеет следующий синтаксис:

http://localhost:8080/verify

```
{
"SignData":"<Электронная подпись документа (BASE64)>",
"DetachedData ":"<Отделенная информация (BASE64)>"
}
```

3.2.4. ШИФРОВАНИЕ ФАЙЛА

Для шифрования информационного сообщения используется функция «encrypt», имеющая следующий синтаксис:

http://localhost:8080/encrypt

```
{
"Certificates": [
        {
        "Certificate":"<Сертификат ЭП (BASE64)>",
        "Certificate":"<Сертификат ЭП (BASE64)>"
        }
],
"Data":"<Шифруемая информация>"
}
```

Если шифрование информационного сообщения осуществляется для одного получателя, и требуется ввести только один сертификат, синтаксис функции «encrypt» выглядит следующим образом:

http://localhost:8080/encrypt

```
{
"Certificates": [
        {
        "Certificate":"<Сертификат ЭП (BASE64)>"
        }
],
"Data":"<Шифруемая информация>"
}
```

Входными параметрами для данной функции являются:

«Certificate»	Сертификат ЭП (BASE64)
«Data»	Шифруемая информация

Возвращаемое значение - результат шифрования:

«EncryptData»	Зашифрованная информация (BASE64)

3.2.5. РАСШИФРОВЫВАНИЕ ФАЙЛА

Для расшифровывания информационного сообщения используется функция «decrypt», имеющая следующий синтаксис:

http://localhost:8080/decrypt

{
"EncryptData ":"<Зашифрованная информация (BASE64)>"
}

Входными параметрами для данной функции являются:

«EncryptData»	Зашифрованная информация (BASE64)

Возвращаемые значения – результат расшифровывания и массив структур «CertInfos»:

«CertInfo»	
«CertBody»	Сертификат (BASE64)
«IssuerInfo»	Сведения о издателе сертификата(BASE64)
«IssuerInfoCn»	
«SerialNumber»	Серийный номер сертификата (BASE64)
«SubjectInfoCn»	Общее имя владельца сертификата
«TimeNotAfter»	Дата истечения сертификата
«TimeNotBefore»	Дата начала действия сертификата

«DecryptCert»	Сертификат (BASE64)
«DecryptData»	Расшифрованная информация (BASE64)

3.2.6. ЗАПРОСЫ DVCS

Для создания запроса в DVCS сервис с целью проверки электронной подписи или действительности сертификата ключа проверки электронной подписи используется функция «dvcs», имеющая следующий синтаксис:

http://localhost:8080/dvcs

{

"ServiceAddress":"<Адрес ДТС сервиса>",

"TransactionID":"<Идентификатор транзакции (GUID)>",

"Certificare":"<Сертификат>",

"SignData":"<Подпись>",

"DetachedData":"<Отделенная информация>",

"Username":"<Имя пользователя в сервисе ДТС>",

"Password":"<Пароль пользователя в сервисе ДТС>"

}

Входными параметрами для данной функции являются:

«ServiceAddress»	Адрес ДТС сервиса
«TransactionID»	Идентификатор транзакции (GUID)
«Certificare»	Сертификат (BASE64)
«SignData»	Подпись
«DetachedData»	Отделенная информация
«Username»	Имя пользователя в сервисе ДТС
«Password»	Пароль пользователя в сервисе ДТС

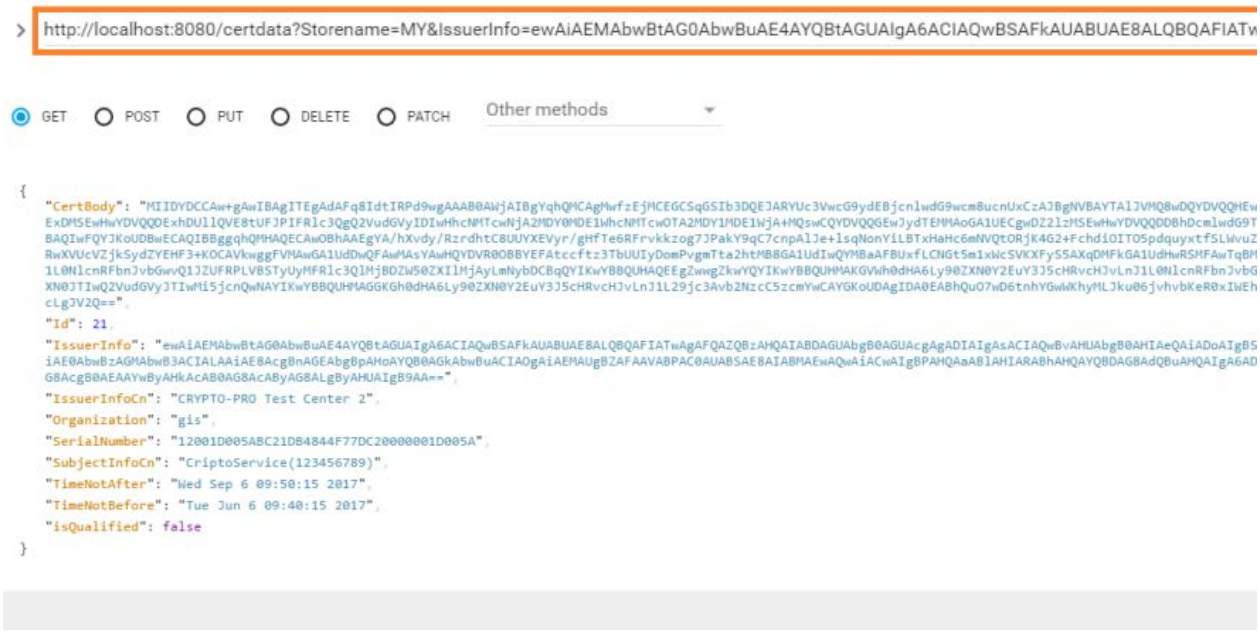
Возвращаемое значение - массив структур DVCSInfos

Структура DVCSInfos	
«CertEncoded»	Сертификат ЭП (BASE64)
«SignatureIndex»	Порядковый номер проверяемой подписи (Числовое значение)
«SignatureTime»	Время подписи (Структура SignatureTime)
«VerifyCertificateResult»	Результат проверки сертификата (True/False)
«VerifyResult»	Результат проверки подписи (True/False)
«StatusString»	Общие сведения о ДТС сервере (Строка)

Структура «SignatureTime»	
«wDay»	День (Числовое значение)
«wDayOfWeek»	День недели (Числовое значение)
«wHour»	Час (Числовое значение)
«wMilliseconds»	Миллисекунда (Числовое значение)
«wMinute»	Минута (Числовое значение)
«wMonth»	Месяц (Числовое значение)
«wSecond»	Секунда (Числовое значение)
«wYear»	Год (Числовое значение)

ПРИЛОЖЕНИЕ 1

Получение сертификата из хранилища с использованием «Advanced REST client».



Создание ЭП информационного сообщения с использованием «Advanced REST client».