Программный комплекс «Блокхост-ЭЦП» 2.0 (ПК «Litoria Desktop»)

Руководство пользователя ДТС клиент

АННОТАЦИЯ

В документе приводится руководство пользователя работы с функциями ДТС клиента в программном комплексе «Блокхост-ЭЦП» 2.0 (в дальнейшем ПК «Litoria Desktop», ПК или комплекс).

В разделе «Назначение ДТС клиента» приводятся сведения о функциях ДТС клиента в комплексе.

В разделе «Условия применения ПК «Litoria Desktop» указаны условия, необходимые для использования комплекса, требования к аппаратным средствам автоматизированного рабочего места (АРМ).

В разделе «Получение личного сертификата и ключевой информации к нему» приведена информация о способах получения личного сертификата и регистрации его на сервере ДТС.

В разделе «Формирование DVCS-запросов» описаны действия, которые необходимо выполнить для создания DVCS-запросов разных типов.

В разделе «Анализ DVC-квитанции» представлено описание информации, отображающейся в получаемой DVC-квитанции.

СОДЕРЖАНИЕ

1. Описание функции «ДТС клиент» 4
2. Условия применения 5
2.1. Требования к программному обеспечению 5
2.2. Требования к техническим средствам 5
2.2.1. Системные требования ОС Windows XP 5
2.2.2. Системные требования ОС Windows Vista 5
2.2.3. Системные требования ОС Windows 7 6
2.2.4. Системные требования ОС Windows 8 6
3. Получение личного сертификата и ключевой информации к нему 7
4. Формирование DVCS-запросов 8
4.1. Создание DVCS-запроса типа VSD 8
4.2. Создание DVCS-запроса типа VPKC 10
5. Анализ DVC-квитанций 14
5.1. Ответ на запрос типа VSD 14
5.1.1. Обычный запрос 14
5.1.2. Анонимный запрос 16
5.2. Ответ на запрос типа VPKC 17
5.2.1. Обычный запрос 17
5.2.2. Анонимный запрос 20

1. ОПИСАНИЕ ФУНКЦИИ «ДТС КЛИЕНТ»

Функция «ДТС клиент» в ПК «Litoria Desktop» позволяет формировать DVCS-запросы 2-х типов:

- подтверждение электронной подписи (ЭП) электронного документа (Validation of Digitally Signed Document – VSD);
- подтверждение действительности сертификата ключа подписи (Validation of Public Key Certificates – VPKC).

Подписанный указанным личным сертификатом DVCS-запрос отправляется для проверки на сервер службы ДТС (**http://росдтс.рф** или **https://rusttp.ru**). Ответ сервера приходит в виде квитанции.

При формировании DVCS-запроса типа VSD можно отправить внутри запроса не документ, а его хэш-значение (применяется, когда недопустима передача содержания конфиденциального документа в канал связи).

Комплекс позволяет создать анонимный DVCS-запрос, но в таком случае квитанция не имеет юридического значения. Анонимный DVCS-запрос используется только в демонстрационных целях.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

ПК «Litoria Desktop» функционирует под управлением следующих ОС:

- Windows XP (32 бит/64 бит);
- Windows Server 2003 (32 бит/64 бит);
- Windows Server 2008 (32 бит/64 бит);
- Windows Vista (32 бит/64 бит);
- Windows 7 (32 бит/64 бит);
- Windows Server 2008 R2;
- Windows 8 (32 бит/64 бит);
- Windows Server 2012 (64 бит);
- Windows 8.1 (32 бит/64 бит);
- Windows Server 2012 R2 (64 бит).

Дополнительно должно быть установлено следующее программное обеспечение:

1. Средство криптографической защиты информации (СКЗИ), реализованное в соответствии с технологией Microsoft CSP. Например: либо программные СКЗИ – «ViPNet CSP» версии 3.2, «ВАЛИДАТА CSP» версии 4.0, «Крипто-Ком 3.2», «КриптоПро CSP» версии 3.6 и выше или ПК «ЛИССИ-CSP»; либо драйвера для аппаратных СКЗИ – «Криптотокен» в составе изделия «eToken ГОСТ» или «РУТОКЕН ЭЦП».

2.2. ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ

Требования к рабочей станции, на которую устанавливается ПК «Litoria Desktop», обусловлены применением ОС.

2.2.1. СИСТЕМНЫЕ ТРЕБОВАНИЯ ОС WINDOWS XP

Минимальные требования к оборудованию для установки Windows XP:

- процессор Pentium с частотой 233 МГц или более быстрый (рекомендуется не менее 300 МГц);
- не менее 64 МБ оперативной памяти (рекомендуется не менее 128 МБ);
- не менее 1,5 ГБ свободного места на жестком диске;
- видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 800x600 точек.

2.2.2. СИСТЕМНЫЕ ТРЕБОВАНИЯ ОС WINDOWS VISTA

Рекомендуемые минимальные требования к оборудованию для использования основных функций Windows Vista Home Basic:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 800 МГц;
- 512 МБ оперативной памяти;
  Примечание. В конфигурациях системы, в которых системная память используется в качестве видеопамяти, после выделения памяти для графики для операционной системы должно быть доступно не менее 448 МБ.
- графическая плата с поддержкой DirectX 9;
- 32 МБ видеопамяти;
- жесткий диск объемом 20 ГБ с 15 ГБ свободного места.

Рекомендуемые минимальные требования к оборудованию для использования основных функций Windows Vista Home Premium, Windows Vista Business, Windows Vista Enterprise и Windows Vista Ultimate:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц;

- 1 ГБ оперативной памяти;
- графическая плата с поддержкой Windows Aero;
  Примечание. Это видеокарта класса DirectX 9 с поддержкой:
  - драйвера WDDM;
  - пиксельных шейдеров версии 2.0 на уровне оборудования;
  - 32 разряда для одного пикселя.
- видеопамяти объемом 128 МБ (минимально);
- жесткий диск объемом 40 ГБ с 15 ГБ свободного места (15 ГБ необходимы для хранения временных файлов во время установки или обновления системы).

2.2.3. СИСТЕМНЫЕ ТРЕБОВАНИЯ ОС WINDOWS 7

Необходимые условия для запуска Windows 7 на компьютере:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- 1 ГБ (для 32-разрядной системы) или 2 ГБ (для 64-разрядной системы) оперативной памяти;
- 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM версии 1.0 или выше.

2.2.4. СИСТЕМНЫЕ ТРЕБОВАНИЯ ОС WINDOWS 8

Необходимые условия для запуска Windows 8 на компьютере:

- процессор с тактовой частотой 1 ГГц или выше с поддержкой PAE, NX и SSE2;
- 1 ГБ (для 32-разрядной системы) или 2 ГБ (для 64-разрядной системы) оперативной памяти;
- 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске;
- графическое устройство Microsoft DirectX 9 с драйвером WDDM.

3. ПОЛУЧЕНИЕ ЛИЧНОГО СЕРТИФИКАТА И КЛЮЧЕВОЙ ИНФОРМАЦИИ К НЕМУ

При создании запроса не анонимного вида потребуется личный цифровой сертификат, зарегистрированный ранее на сервере ДТС.

Цифровой сертификат содержит идентификационную информацию о пользователе (в том числе его имя), открытый ключ и уникальную цифровую подпись, которая закрепляет сертификат за удостоверяющим центром (УЦ), который его создал. Закрытый ключ, соответствующий открытому ключу сертификата, должен находиться в контейнере на отчуждаемом носителе. В качестве отчуждаемого носителя может использоваться любой носитель (например, дискета 3,5", сменный носитель с интерфейсом USB и др.)

С помощью ПК «Litoria Desktop» вы можете создать запрос, который затем отправите на рассмотрение в УЦ, и на основе которого УЦ выпустит для вас личный цифровой сертификат. Также можно получить отчуждаемый носитель с личным сертификатом в любом аккредитованном Удостоверяющем Центре (УЦ).

После получения сертификата установите его в хранилище сертификатов «Личное».

Установить личный сертификат в хранилище сертификатов «Личное» можно несколькими способами:

- с помощью стандартного интерфейса ПК «Litoria Desktop» (действия описаны в документе «ПК «Litoria Desktop». Руководство пользователя (стандартный интерфейс)»);
- с помощью СКЗИ, установленного на компьютере пользователя.

Для регистрации личного сертификата на сервере ДТС сообщите об этом менеджеру УЦ при получении сертификата.

Перед выполнением операций с отчуждаемым носителем, который будет содержать ключевую информацию и сертификат, обязательно ознакомьтесь с документом «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных № 149/6/6-622».

4. ФОРМИРОВАНИЕ DVCS-ЗАПРОСОВ

4.1. СОЗДАНИЕ DVCS-ЗАПРОСА ТИПА VSD

1. Откройте стандартный интерфейс ПК «Litoria Desktop».

2. Выберите операцию *«ДТС клиент»*.

3. Появится окно *«ДТС клиент»* (Рисунок 4.1).

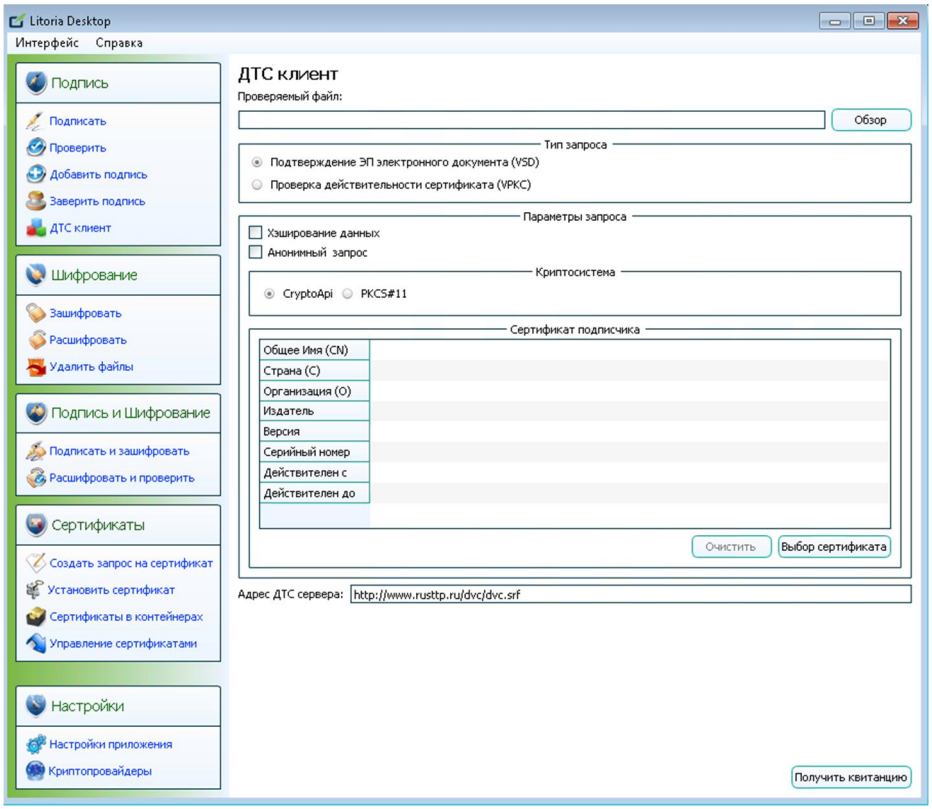

Рисунок 4.1

4. Нажмите на кнопку *«Обзор»*.

5. В открывшемся окне *«Укажите подписанный файл»* выберите файл, подпись которого вы хотите проверить, и нажмите на кнопку *«Открыть»*.

6. В окне *«ДТС клиент»* в поле *«Проверяемый файл»* отобразится путь и имя выбранного файла.

7. При использовании физического отчуждаемого носителя для подписи запроса вставьте его в нужный разъем.

8. В области *«Тип запроса»* проверьте, правильно ли указан тип запроса. Должен быть выбран пункт *«Подтверждение ЭЦП электронного документа (VSD)»*.

9. Установите параметры запроса. В таблице 4.1 указаны виды запроса типа VSD и параметры, установка которых необходима для создания запроса.

Таблица 4.1

Виды запроса VSD	**Параметры запроса в ПК «Litoria Desktop»**	**Примечание**
Обычный запрос	Криптосистема; Сертификат подписчика.	Флаги не надо устанавливать.
Обычный запрос с хэшированием данных.	Хэширование данных; Криптосистема; Сертификат подписчика.	

Виды запроса VSD	Параметры запроса в ПК «Litoria Desktop»	Примечание
Анонимный запрос	Анонимный запрос.	Используется только в демонстрационных целях.
Анонимный запрос с хэшированием данных.	Хэширование данных; Анонимный запрос.	

10. Укажите криптосистему – *«CryptoApi»* (при использовании программного криптопровайдера, например: «ViPNet CSP» версии 3.2; «КриптоПро CSP» версии 3.6 или выше) или *«PKCS#11»* (при использовании аппаратного криптопровайдера, например: «eToken ГОСТ» или «РУТОКЕН ЭЦП»).

11. Для указания сертификата подписчика нажмите на кнопку *«Выбор сертификата»*.

12. Появится окно *«Список сертификатов»* с вашими личными сертификатами. В появившемся окне отображается статус сертификатов, а также здесь можно провести проверку сертификата по всем параметрам (см. в документе «Руководство пользователя» раздел 3.3.6), просмотреть его содержимое и путь сертификации.

13.В появившемся окне *«Список сертификатов»* выберите свой личный сертификат, который ранее был зарегистрирован на сервере ДТС, и нажмите на кнопку *«Выбрать»*.

14.В окне *«ДТС клиент»* в области *«Сертификат подписчика»* отобразится информация выбранного сертификата.

15.В поле *«Адрес ДТС сервера»* по умолчанию указан *«http://www.rusttp.ru/dvc/dvc.srf»*. Если будет использоваться другой ДТС сервер, введите нужный адрес.

16.Для отправки запроса и получения квитанции нажмите на кнопку *«Получить квитанцию»*.

17.Если ранее была указана криптосистема *«PKCS#11»*, то появится окно со списком подключенных аппаратных криптопровайдеров в момент выполнения операции (Рисунок 4.2).

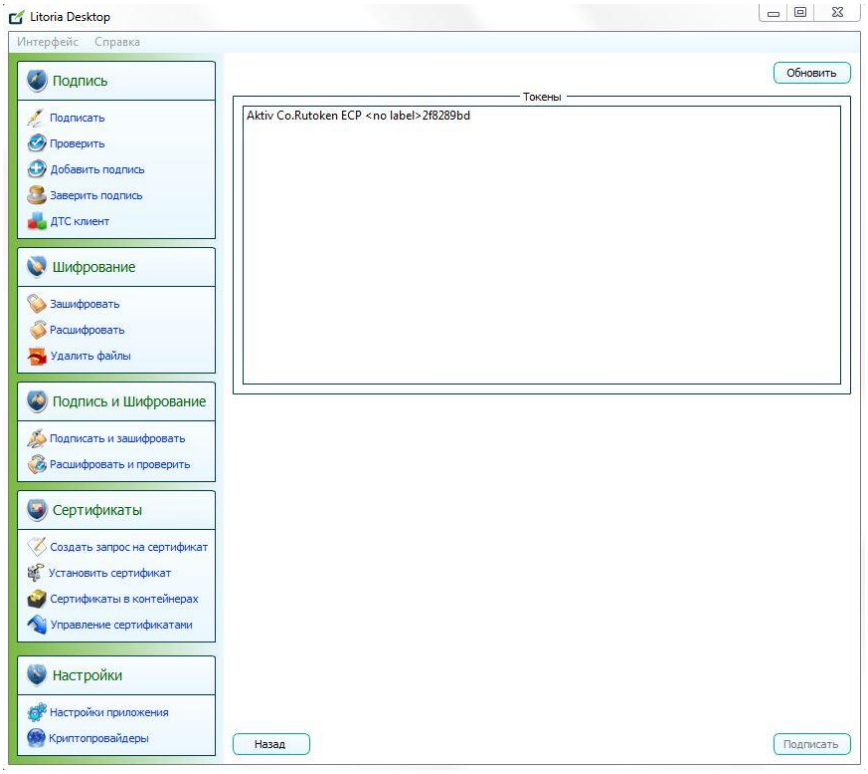

Рисунок 4.2

18.Выберите из списка название используемого устройства и нажмите на кнопку *«Получить квитанцию»*.

19.Если ранее не был сохранен pin-код к ключевому носителю, то возможно появление окна с запросом ввести pin-код к контейнеру закрытого ключа. Введите pin-код и нажмите на кнопку *«Ок»*.

20.После выполнения операции открывается окно *«Результаты отправки запроса ДТС»*, в котором отображена информация DVC-квитанции (Рисунок 4.3).

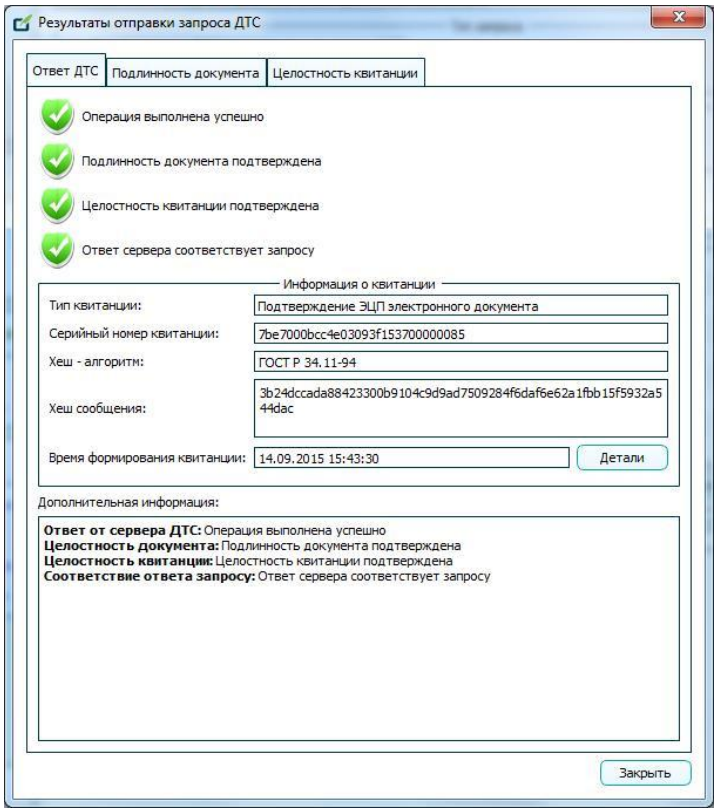

Рисунок 4.3

4.2. СОЗДАНИЕ DVCS-ЗАПРОСА ТИПА VPKC

1. Откройте стандартный интерфейс ПК «Litoria Desktop».

2. Выберите операцию *«ДТС клиент»*.

3. Появится окно *«ДТС клиент»* (Рисунок 4.4).

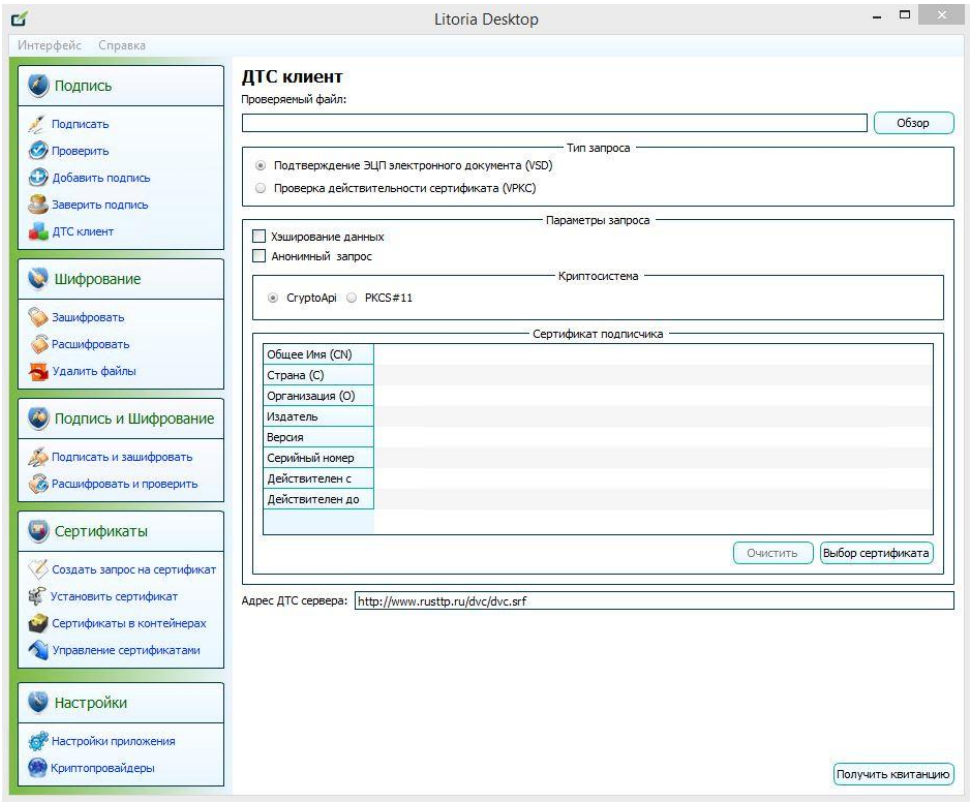

Рисунок 4.4

4. Нажмите на кнопку *«Обзор»*.

5. В открывшемся окне *«Укажите подписанный файл»* выберите файл сертификата, действительность которого вы хотите проверить, и нажмите на кнопку *«Открыть»*.

6. В окне *«ДТС клиент»* в поле *«Проверяемый файл»* отобразится путь и имя выбранного файла.

7. При использовании физического отчуждаемого носителя для подписи запроса вставьте его в нужный разъем.

8. В области *«Тип запроса»* установите переключатель *«Проверка действительности сертификата (VPKC)»*.

9. Установите параметры запроса. В таблице 4.2 указаны виды запроса типа VPKC и параметры, установка которых необходима для создания запроса.

Таблица 4.2

Виды запроса VPKC	**Параметры запроса в ПК «Litoria Desktop»**	**Примечание**
Обычный запрос	Криптосистема; Сертификат подписчика.	Флаги не надо устанавливать.
Анонимный запрос	Анонимный запрос.	Используется только в демонстрационных целях.

10. Укажите криптосистему – *«CryptoApi»* (при использовании программного криптопровайдера, например: «ViPNet CSP» версии 3.2; «КриптоПро CSP» версии 3.6 или выше) или *«PKCS#11»* (при использовании аппаратного криптопровайдера, например: «eToken ГОСТ» или «РУТОКЕН ЭЦП»).

11. Для указания сертификата подписчика нажмите на кнопку *«Выбор сертификата»*.

12. Появится окно *«Список сертификатов»* с вашими личными сертификатами. В появившемся окне отображается статус сертификатов, а также здесь можно провести проверку сертификата по всем параметрам (см. в документе «Руководство пользователя» раздел 3.3.6), просмотреть его содержимое и путь сертификации.

13. В появившемся окне *«Список сертификатов»* выберите свой личный сертификат, который ранее был зарегистрирован на сервере ДТС, и нажмите на кнопку *«Выбрать»*.

14. В окне *«ДТС клиент»* в области *«Сертификат подписчика»* отобразится информация выбранного сертификата.

15. В поле *«Адрес ДТС сервера»* по умолчанию указан *«http://www.rusttp.ru/dvc/dvc.srf»*. Если будет использоваться другой ДТС сервер, введите нужный адрес.

16. Для отправки запроса и получения квитанции нажмите на кнопку *«Получить квитанцию»*.

17. Если ранее была указана криптосистема *«PKCS#11»*, то появится окно со списком подключенных аппаратных криптопровайдеров в момент выполнения операции (Рисунок 4.5).

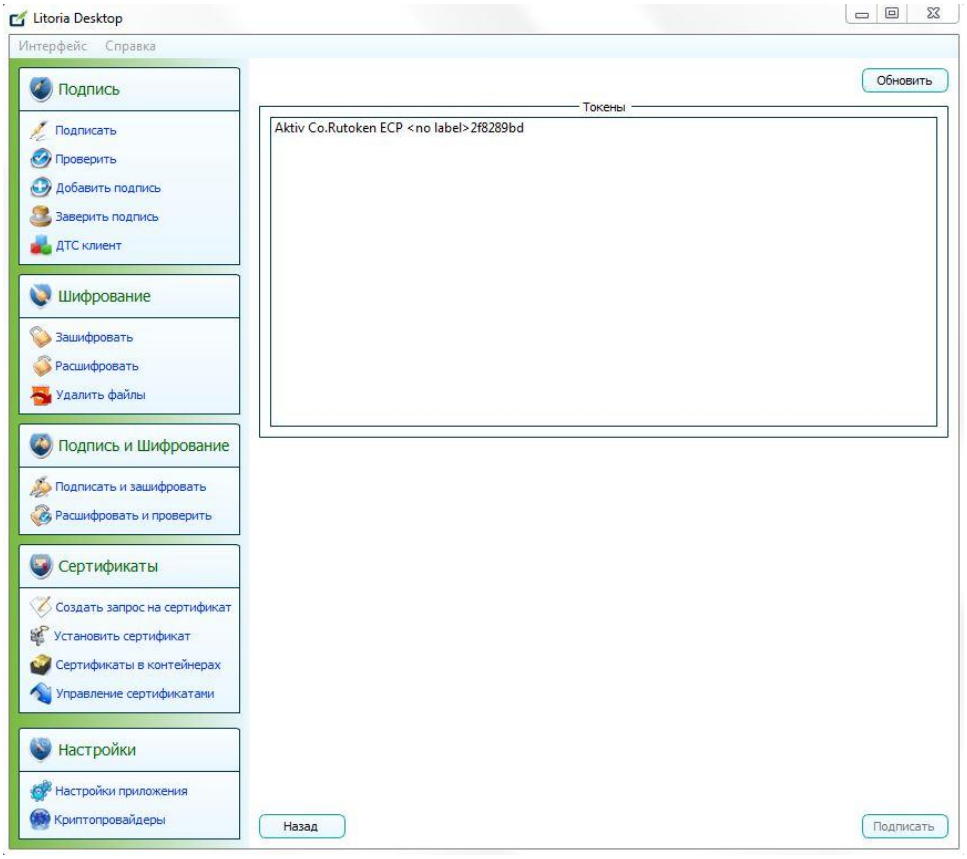

Рисунок 4.5

18. Выберите из списка название используемого устройства и нажмите на кнопку *«Получить квитанцию»*.

19. Если ранее не был сохранен pin-код к ключевому носителю, то возможно появление окна с запросом ввести pin-код к контейнеру закрытого ключа. Введите pin-код и нажмите на кнопку *«Ок»*.

20. После выполнения операции открывается окно *«Результаты отправки запроса ДТС»*, в котором отображена информация DVC-квитанции (Рисунок 4.6).

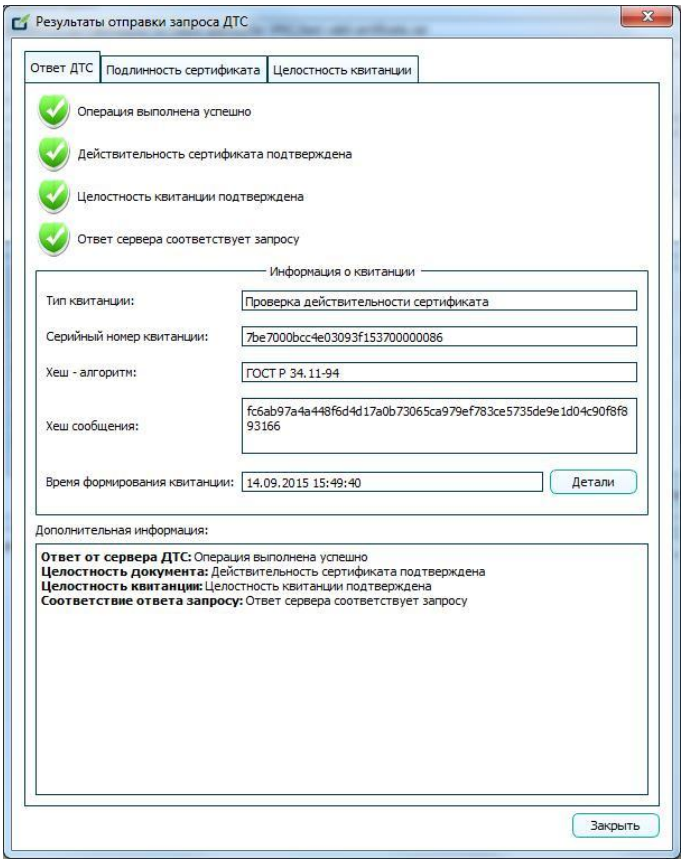
Результаты отправки запроса ДТС
Ответ ДТС
Подлинность сертификата
Целостность квитанции
Операция выполнена успешно
Действительность сертификата подтверждена
Целостность квитанции подтверждена
Ответ сервера соответствует запросу
Информация о квитанции
Тип квитанции:
Проверка действительности сертификата
Серийный номер квитанции:
7be7000bcc4e03093f153700000086
Хеш - алгоритм:
ГОСТ Р 34.11-94
Хеш сообщения:
fc6ab97a4a448f6d4d17a0b73065ca979ef783ce5735de9e1d04c90f8f893166
Время формирования квитанции:
14.09.2015 15:49:40
Детали
Дополнительная информация:
Ответ от сервера ДТС: Операция выполнена успешно
Целостность документа: Действительность сертификата подтверждена
Целостность квитанции: Целостность квитанции подтверждена
Соответствие ответа запросу: Ответ сервера соответствует запросу
Закрыть

Рисунок 4.6

5. АНАЛИЗ DVC-КВИТАНЦИЙ

После выполнения операции отправки запроса любого типа в ПК «Litoria Desktop» открывается окно *«Результаты отправки запроса ДТС»*, в котором отображена DVC-квитанция.

Содержание DVC-квитанции для разных типов запросов отличается друг от друга. Ниже будет представлено описание этого содержания.

5.1. ОТВЕТ НА ЗАПРОС ТИПА VSD

5.1.1. ОБЫЧНЫЙ ЗАПРОС

На рисунке 5.1 представлена DVC-квитанция, полученная в ответ на обычный запрос типа VSD. По умолчанию открыта вкладка *«Ответ ДТС»*.

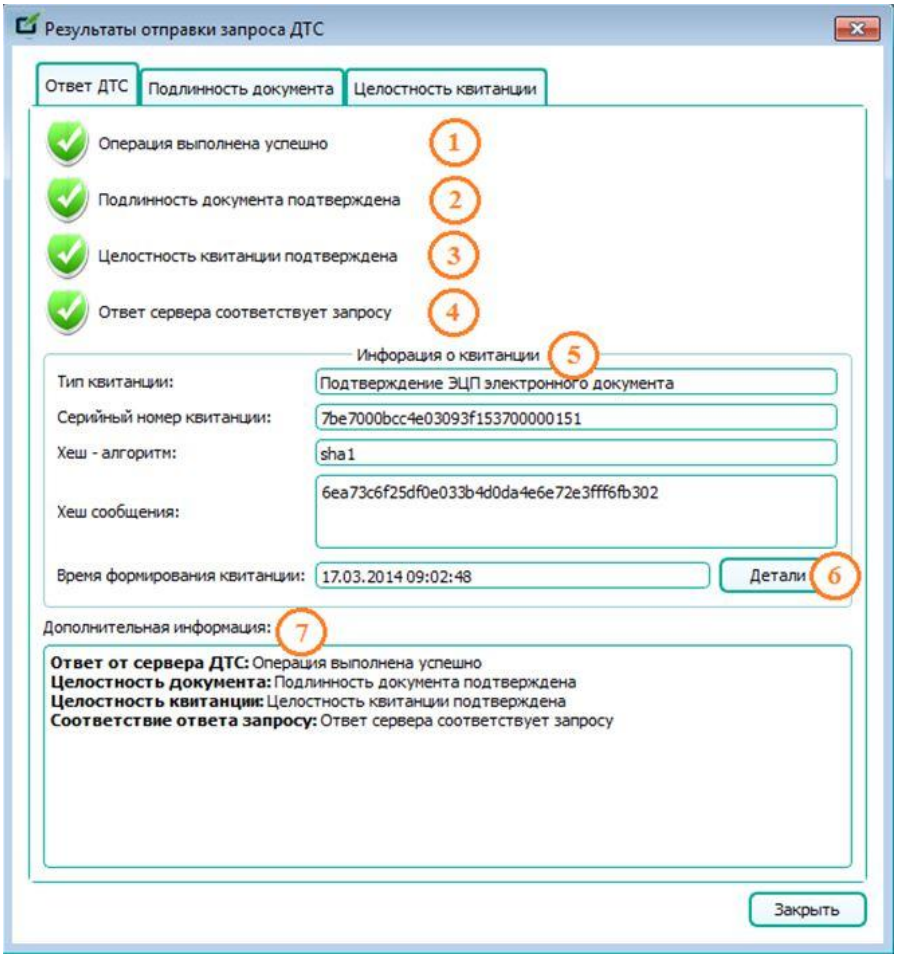

Рисунок 5.1. Вкладка *«Ответ ДТС»*

Описание компонентов вкладки *«Ответ ДТС»*, отмеченных на рисунке 5.1:

1. Результат выполнения операции;
2. Статус подтверждения подлинности документа;
3. Статус подтверждения целостности квитанции;
4. Статус соответствия ответа сервера запросу;
5. Информация о полученной квитанции;
6. Кнопка *«Детали»*, при нажатии на которую открывается окно *«Детальная информации о штампе времени»* (Рисунок 5.2);
7. Поле *«Дополнительная информация»*, которое дублирует информацию п.п.1-3 и в случае отрицательного результата одной или нескольких проверок отображает подробное описание ошибки.

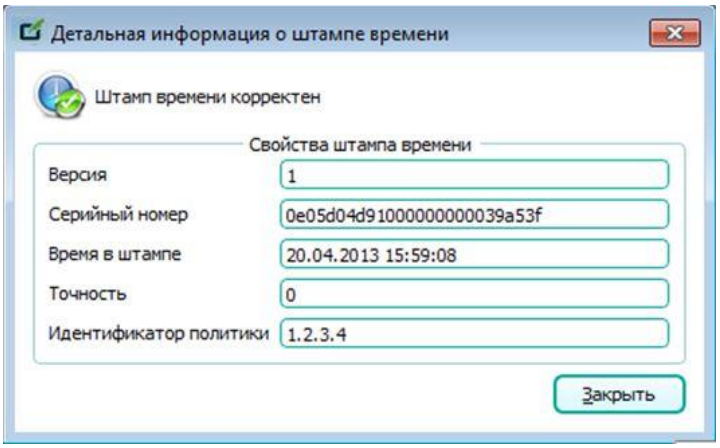

Рисунок 5.2

На рисунке 5.3 представлен вид вкладки *«Подлинность документа»*.

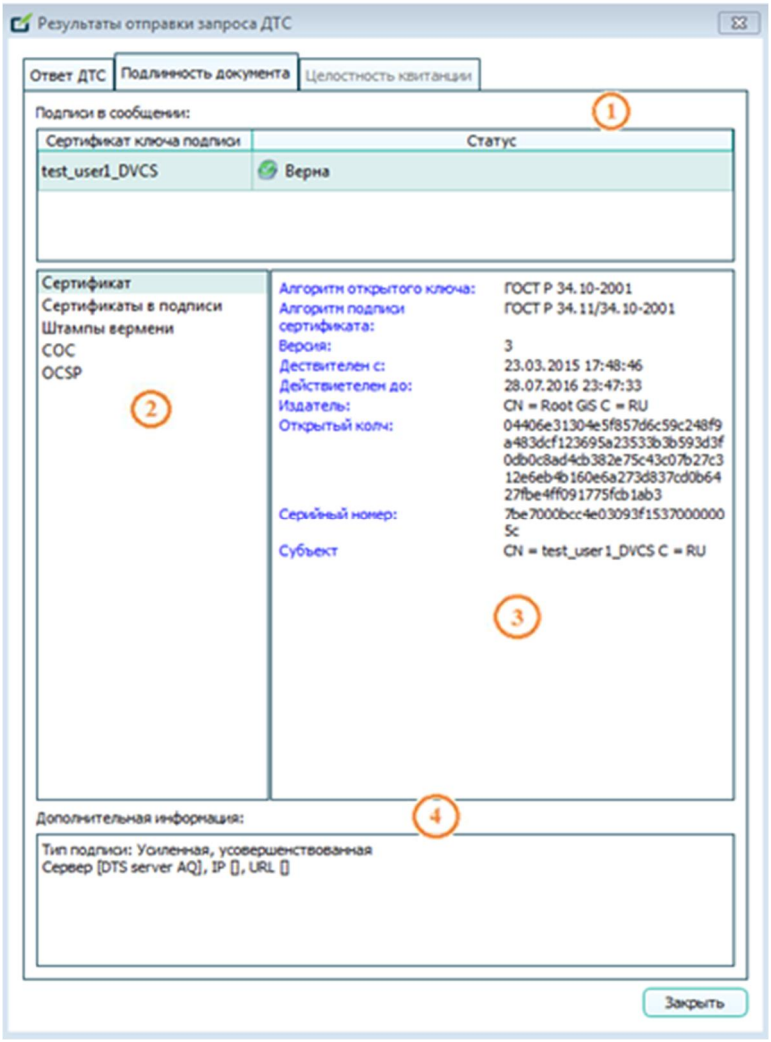

Рисунок 5.3. Вкладка *«Подлинность документа»*

Описание компонентов вкладки *«Подлинность документа»*, отмеченных на рисунке 5.3:

1. Состав подписей, находящихся в проверяемом файле, и их статус;
2. Вкладки *«Сертификат»*, *«Сертификат в подписи»*, *«Штампы времени»*, *«COC»*, *«OCSP»*;
3. Подробное описание содержания подписи в зависимости от вкладки, выбранной в разделе 2: сертификат подписчика; сертификаты, участвующие в создании этой подписи; штампы времени; списки отзыва сертификатов; OCSP ответы;

4. Поле *«Дополнительная информация»*, в котором отображается информация о типе подписи и месте создания квитанции.

На рисунке 5.4 представлен вид вкладки *«Целостность квитанции»*.

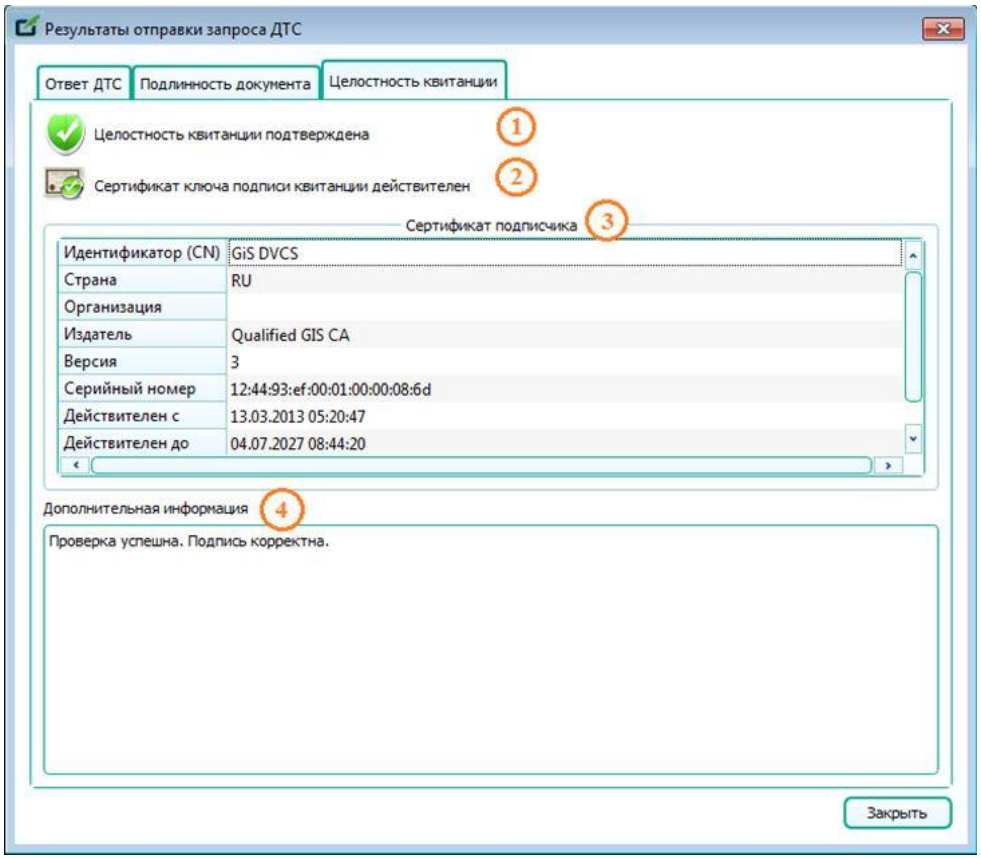

Рисунок 5.4. Вкладка *«Целостность квитанции»*

Описание компонентов вкладки *«Целостность квитанции»*, отмеченных на рисунке 5.4:

1. статус подтверждения целостности квитанции;
2. статус сертификата ключа подписи квитанции;
3. информация о сертификате, которым была подписана квитанция;
4. поле *«Дополнительная информация»*, в котором отображается информация о результатах операции и статусе подписи квитанции.

5.1.2. АНОНИМНЫЙ ЗАПРОС

DVC-квитанция, полученная в ответ на анонимный запрос типа VSD (Рисунок 5.5), отличается от DVC-квитанции, полученной на обычный запрос, следующем:

1. Не имеет юридического значения;
2. Не имеет подписи создателя квитанции;
3. Используется только в демонстрационных целях.

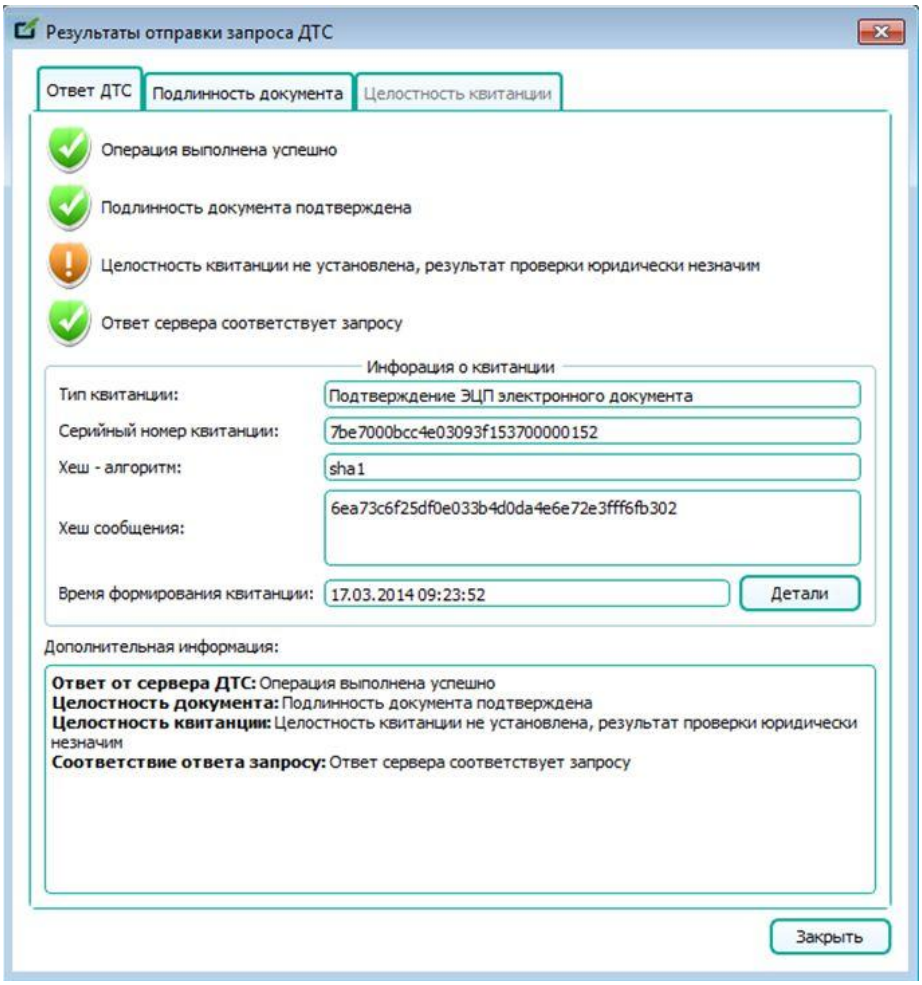

Рисунок 5.5

5.2. ОТВЕТ НА ЗАПРОС ТИПА VPKC

5.2.1. ОБЫЧНЫЙ ЗАПРОС

На рисунке 5.6 представлена DVC-квитанция, полученная в ответ на обычный запрос типа VPKC. По умолчанию открыта вкладка *«Ответ ДТС»*.

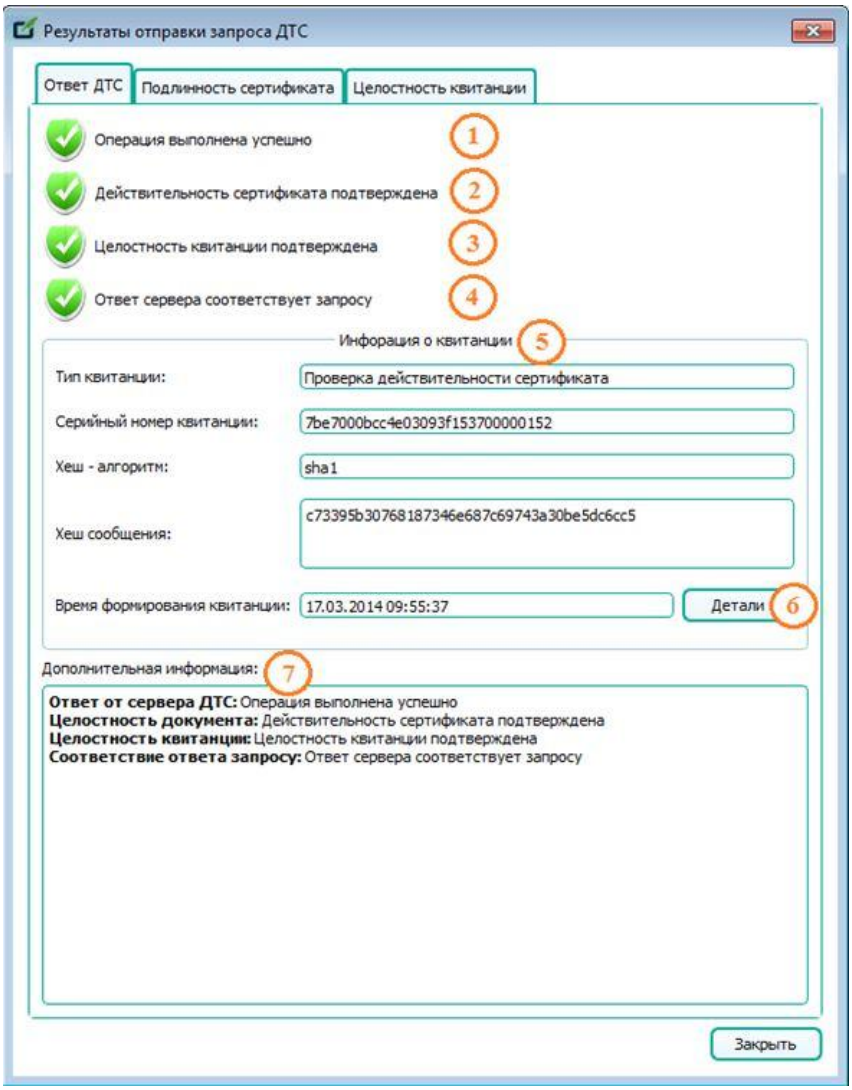

Рисунок 5.6. Вкладка *«Ответ ДТС»*

Описание компонентов вкладки *«Ответ ДТС»*, отмеченных на рисунке 5.6:

1. Результат выполнения операции;
2. Статус проверяемого сертификата;
3. Статус подтверждения целостности квитанции;
4. Статус соответствия ответа сервера запросу;
5. Информация о полученной квитанции;
6. Кнопка *«Детали»*, при нажатии на которую открывается окно *«Детальная информации о штампе времени»*;
7. Поле *«Дополнительная информация»*, которое дублирует информацию п.п.1-3 и в случае отрицательного результата одной или нескольких проверок отображает подробное описание ошибки.

На рисунке 5.7 представлен вид вкладки *«Подлинность сертификата»*.

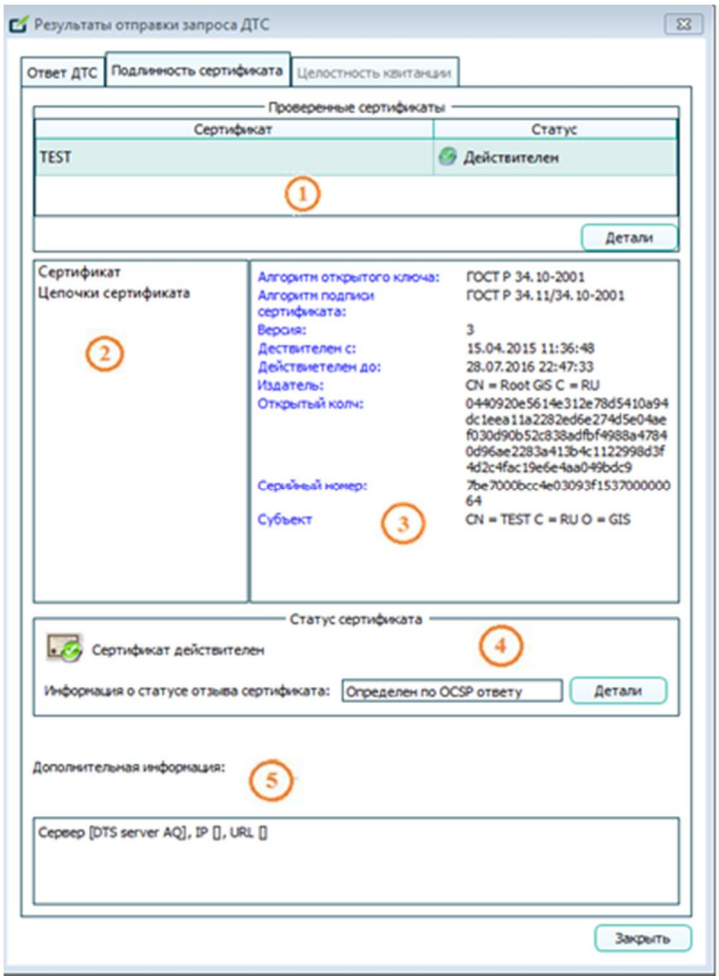

Рисунок 5.7. Вкладка *«Подлинность сертификата»*

Описание компонентов вкладки *«Подлинность сертификата»*, отмеченных на рисунке 5.6:

1. Проверенные сертификаты и их статус;
2. Вкладки *«Сертификат»* и *«Цепочки сертификации»*;
3. Сведения о сертификате (при включенной вкладке *«Сертификат»*) или сертификаты, состоящие в одной цепочке сертификации с проверенным сертификатом (при включенной вкладке *«Цепочки сертификации»*);
4. Статус сертификата и информация о статусе отзыва сертификата;
5. Поле *«Дополнительная информация»*, в котором отображается информация о месте создания квитанции.

На рисунке 5.8 представлен вид вкладки *«Целостность квитанции»*.

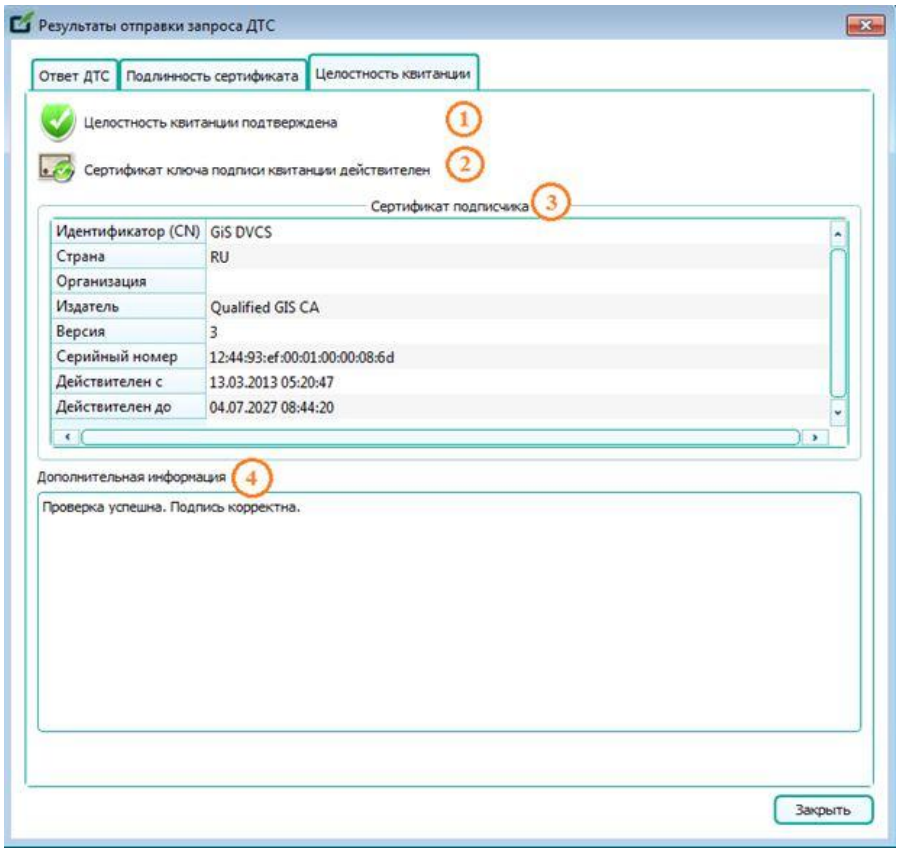

Рисунок 5.8. Вкладка *«Целостность квитанции»*

Описание компонентов вкладки *«Целостность квитанции»*, отмеченных на рисунке 5.8:

1. Статус подтверждения целостности квитанции;
2. Статус сертификата ключа подписи квитанции;
3. Информация о сертификате, которым была подписана квитанция;
4. Поле *«Дополнительная информация»*, в котором отображается информация о результатах операции и статусе подписи квитанции.

5.2.2. АНОНИМНЫЙ ЗАПРОС

DVC-квитанция, полученная в ответ на анонимный запрос типа VPKC (Рисунок 5.9), отличается от DVC-квитанции, полученной на обычный запрос, следующем:

1. Не имеет юридического значения;
2. Не имеет подписи создателя квитанции;
3. Используется только в демонстрационных целях.

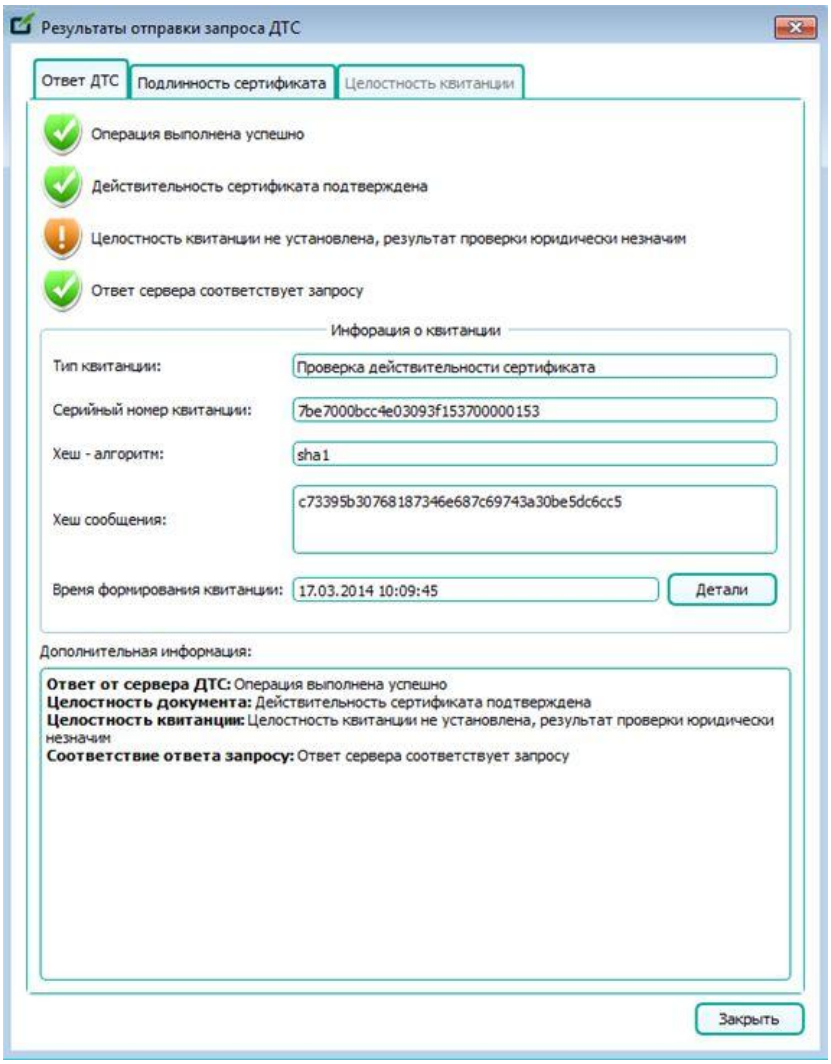
Результаты отправки запроса ДТС
Ответ ДТС
Подлинность сертификата
Целостность квитанции
Операция выполнена успешно
Действительность сертификата подтверждена
Целостность квитанции не установлена, результат проверки юридически незначим
Ответ сервера соответствует запросу
Инфорация о квитанции
Тип квитанции:
Проверка действительности сертификата
Серийный номер квитанции:
7be7000bcc4e03093f153700000153
Хеш - алгоритм:
sha1
Хеш сообщения:
c73395b3076818734 6e687c69743a30be5dc6cc5
Время формирования квитанции:
17.03.2014 10:09:45
Детали
Дополнительная информация:
Ответ от сервера ДТС: Операция выполнена успешно
Целостность документа: Действительность сертификата подтверждена
Целостность квитанции: Целостность квитанции не установлена, результат проверки юридически незначим
Соответствие ответа запросу: Ответ сервера соответствует запросу
Закрыть

Рисунок 5.9