

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1. ТРЕБОВАНИЯ ДЛЯ РАБОТЫ С ПОРТАЛОМ	5
2. ОБЩАЯ ИНФОРМАЦИЯ ПО РАБОТЕ С ПОРТАЛОМ.....	6
3. РАБОТА С DVCS-МОДУЛЕМ.....	8
4. РАБОТА С ХКMS-МОДУЛЕМ.....	19
5. РАБОТА С OASIS DSS-МОДУЛЕМ.....	26
6. ТЕСТИРОВАНИЕ ВНЕШНЕЙ СЛУЖБЫ.....	28
7. ПРИКЛАДОЙ ПРОГРАММНЫЙ ИНТЕРФЕЙС	29

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лист	№	Подп.	Дата		

Руководство пользователя

Лист

2

ВВЕДЕНИЕ

Портал банка спецификаций это ресурс, предназначенного для агрегации существующих технологических и программных решений и нормативно-распорядительных документов с целью их использования при разработке, тестировании и эксплуатации систем взаимного признания электронной подписи для обеспечения юридической значимости трансграничного электронного документооборота между администрациями железных дорог – членами Организации сотрудничества железных дорог (ОСЖД) при организации международных грузовых железнодорожных перевозок.

Настоящий документ предназначен для ознакомления пользователей с возможностями портала и упрощения навигации по нему.

Для корректной работы с порталом должны быть удовлетворены требования, представленные в разделе 1.

Раздел 2 содержит общую информация по работе с порталом, в том числе описание основных структурных элементов портала.

В разделах 3, 4 и 5 подробно рассматривается работа с DVCS-, XKMS- и OASIS DSS-модулями портала.

Раздел 6 посвящён тестированию внешних служб, предоставляющих сервисы доверенной третьей стороны.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
						3
	Лис	№	Подп.	Дата		

Раздел 7 содержит описание формата запросов для доступа к прикладным программным интерфейсам (API) модулей портала.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

1. ТРЕБОВАНИЯ ДЛЯ РАБОТЫ С ПОРТАЛОМ

Портал банка спецификаций является веб-порталом – сайтом в компьютерной сети, поэтому для работы необходимо использовать браузер (веб-обозреватель).

Для корректной работы портала браузер должен поддерживать:

- JavaScript (jQuery 1.11.3);
- Html5;
- Css3.

Рекомендуется использовать последние версии браузеров и платформ:

	Chrome	Firefox	Internet Explorer (8-11)	Opera	Safari
Android	+	+		-	
iOS	+			-	+
Mac OS X	+	+		+	+
Windows	+	+	+	+	-

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
						5
Лист	№	Подп.	Дата			

2. ОБЩАЯ ИНФОРМАЦИЯ ПО РАБОТЕ С ПОРТАЛОМ

Портал является закрытым ресурсом. Для доступа необходимо иметь учётную запись пользователя и пароль. При заходе на страницу портала происходит перенаправление на страницу авторизации (Рисунок 1).

Рисунок 1. Страница авторизации.

Если у Вас имеется логин и пароль для доступа к portalу, то выполните вход и начните работу.

Если у Вас нет логина и пароля для доступа к portalу, то перейдите по ссылке «Регистрация» на странице входа и следуйте дальнейшим указаниям.

Если Вы забыли логин или пароль, то перейдите по ссылке «Забыли логин или пароль?» на странице входа и следуйте дальнейшим указаниям.

Портал имеет несколько разделов:

- Главная

Главная страница портала, где размещена информация общего характера.

Инд. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
Лис	№	Подп.	Дата	6		

- О проекте

На данной странице расположена информация о проекте.

- Спецификации

Данный раздел содержит информация по существующим спецификациям и схемам подключения с описанием.

- Документы

Данный раздел содержит различные документы, необходимые пользователям портала. Другие страницы портала при отсылке к документам ссылаются на документы с этой страницы.

- Контакты

Данный раздел содержит контактную информацию для связи.

- Разработчикам

Данный раздел содержит информацию для разработчиков. На главной странице раздела содержится краткая информация об используемых протоколах. Раздел содержит три подраздела – DVCS, XKMS и OASIS DSS:

- DVCS

Подраздел содержит информацию для организации взаимодействия по протоколу DVCS и состоит из следующих страниц:

- Информация

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

Страница с информацией о протоколе.

- Проверка

Страница содержит форму для проверки присоединённой подписи документа.

- Тестирование сторонней службы

Страница для тестирования сторонней VSD DVCS-службы.

- API

Страница с описанием API – прикладного программного интерфейса, позволяющего воспользоваться функциями портала во внешних программных продуктах.

- Конструктор

Конструктор позволяет наглядно ознакомиться и пройти по ключевым этапам взаимодействия по протоколу

3. Работа с DVCS-модулем

DVCS-модуль осуществляет взаимодействие с DVCS-службой ДТС ОАО «РЖД»

Работа с DVCS-модулем начинается на главной странице раздела «DVCS» (Рисунок 2).

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

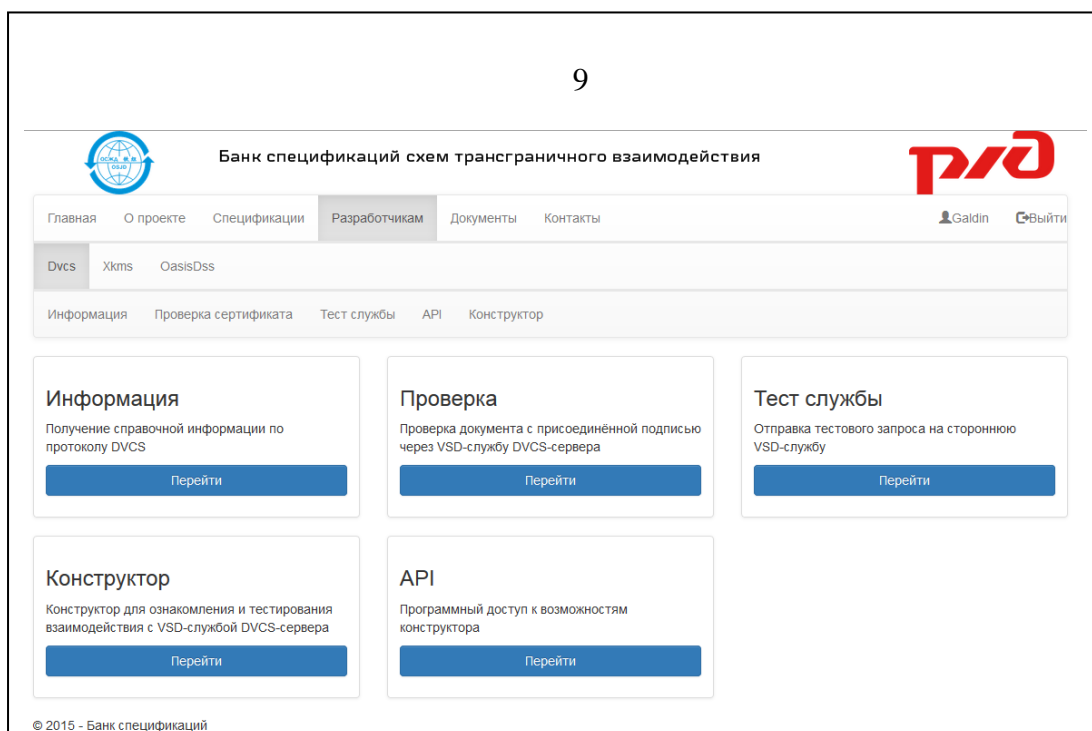


Рисунок 2. Главная страница раздела DVCS.

Страницы «Информация» и «API» носят информационный характер и не взаимодействуют с DVCS-модулем.

Страница «Проверка» позволяет проверить присоединённую подпись документа через DVCS-службу (Рисунок 3).

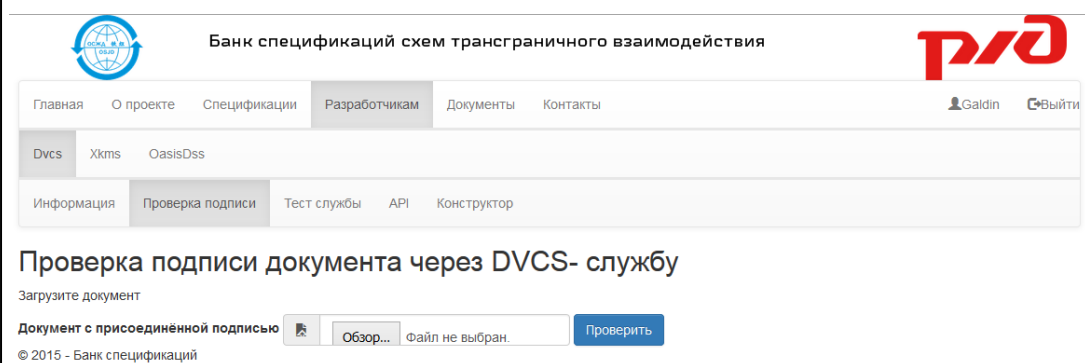


Рисунок 3. Страница проверки подписи документа через DVCS-службу

Для этого необходимо загрузить подписанный документ и нажать на кнопку «проверить». После этого будет сформирован и отправлен запрос на проверку, получен ответ и выведен результат.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата

В случае, если проверка прошла успешно, будет выведена информация об успешной проверке, информация о загруженном файле и информация об ответе службы (Рисунок 4)

Банк спецификаций схем трансграничного взаимодействия

Главная О проекте Спецификации Разработчикам Документы Контакты

Dvcs Xkms OasisDss

Информация Проверка подписи Тест службы API Конструктор

Проверка подписи документа через DVCS- службу

Granted

Загрузите документ

Документ с присоединённой подписью

Информация о файле

Имя	sign_doc.txt
Размер	64665 байт

Информация о сертификате подписи

[Subject] OID.1.2.643.100.1=1027739207462, OID.1.2.643.3.131.1.1=7604190124, E=a.igin@vniias.ru, T=директор, O="ООО ""Рога и копыта""", CN="ООО ""Рога и копыта""", SN=Игин, G=Алексей Георгиевич, L=г. Москва, S=77 Москва, C=RU [Issuer] OID.1.2.643.100.1=1027739207462, OID.1.2.643.3.131.1.1=7604190124, E=a.igin@vniias.ru, T=директор, O="ООО ""Рога и копыта""", CN="ООО ""Рога и копыта""", SN=Игин, G=Алексей Георгиевич, L=г. Москва, S=77 Москва, C=RU [Serial Number] 00B6A61CDC6D774F621209A7CEF24E9B [Not Before] 11.05.2015 12:55:58 [Not After] 12.05.2016 12:54:30 [Thumbprint] A681F57C0E419E4C4A50583A232965183866EFA6

Информация об ответе службы

Статус	Granted
Время запроса (UTC)	18 08 2015 07:05:04
Серийный номер	d749979e-7ea9-4bee-be31-9ad6c1e376db
Номер запроса	B09E3327-D324-460D-B934-063A3AC457D0
Дата запроса (UTC)	18 08 2015 07:00:42
Податель запроса	GeneralNames: 4: CN=DVCS Service 8: 1.2.643.3.37.4.1.1
Тип запроса	VSD

Информация о сертификате подписи ответа

[Subject] E=cainfo@vniias.ru, CN=DVCS Service, O=JSC NIAS, L=Moscow, C=RU [Issuer] CN=CA-NIAS-RSA, OU=HTK ТИО, O="ОАО "НИИАС", L=Москва, S=77 г.Москва, C=RU, E=cainfo@vniias.ru, STREET=ул. Нижегородская 27 стр. 1 [Serial Number] 65940E31000000000006 [Not Before] 27.11.2014 17:04:02 [Not After] 27.11.2015 17:14:02 [Thumbprint] 64DBA9C444524667BD9E10E852B150EAF0BF4308

© 2015 - Банк спецификаций

Рисунок 4. Страница успешной проверки подписи DVCS-службой.

В случае неудачи будет выведено сообщение об ошибке (Рисунок 5)

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лист	№	Подп.	Дата	Руководство пользователя	Лист

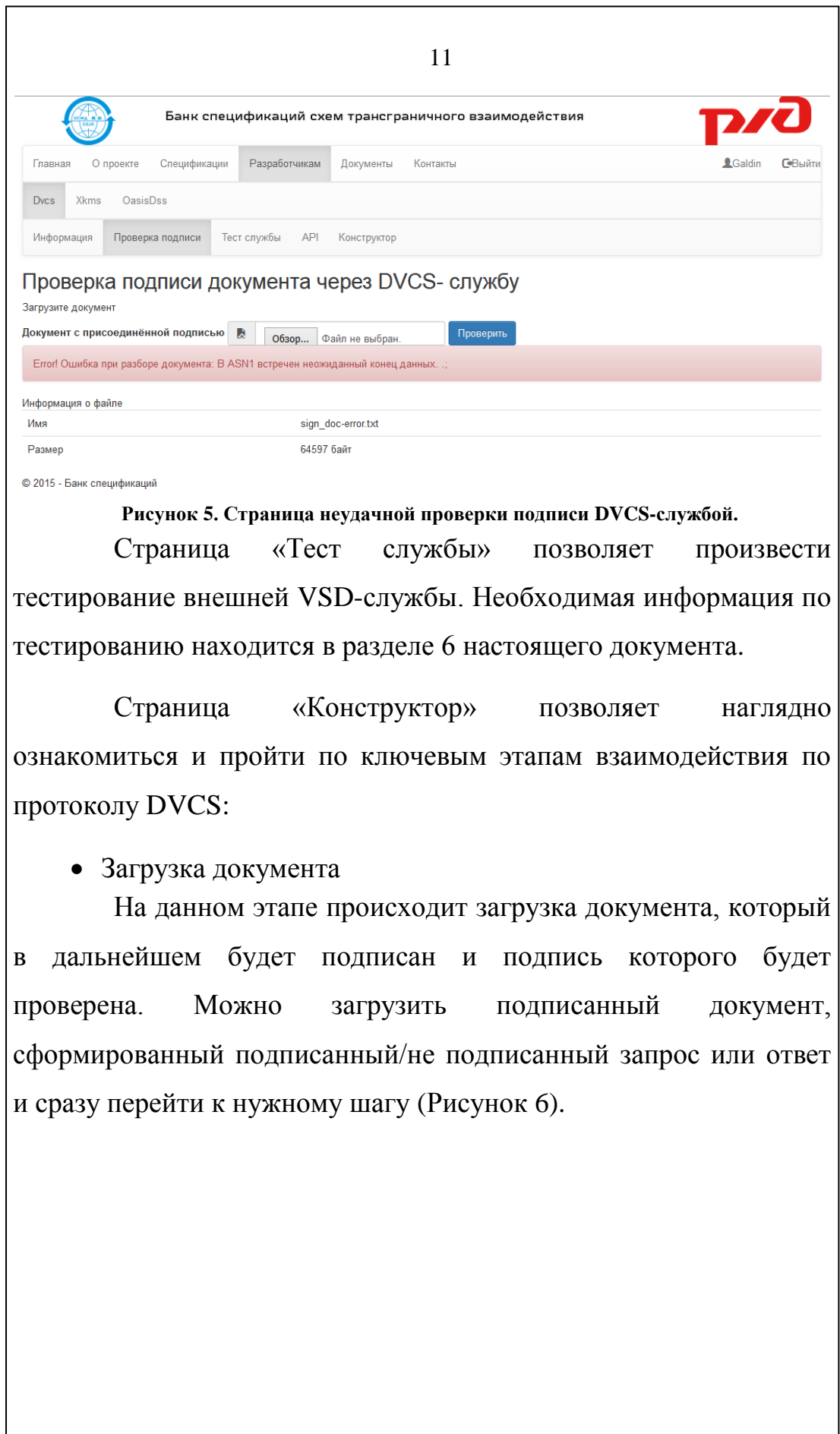


Рисунок 5. Страница неудачной проверки подписи DVCS-службой.

Страница «Тест службы» позволяет произвести тестирование внешней VSD-службы. Необходимая информация по тестированию находится в разделе 6 настоящего документа.

Страница «Конструктор» позволяет наглядно ознакомиться и пройти по ключевым этапам взаимодействия по протоколу DVCS:

- Загрузка документа

На данном этапе происходит загрузка документа, который в дальнейшем будет подписан и подпись которого будет проверена. Можно загрузить подписанный документ, сформированный подписанный/не подписанный запрос или ответ и сразу перейти к нужному шагу (Рисунок 6).

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
Лис	№	Подп.	Дата			11

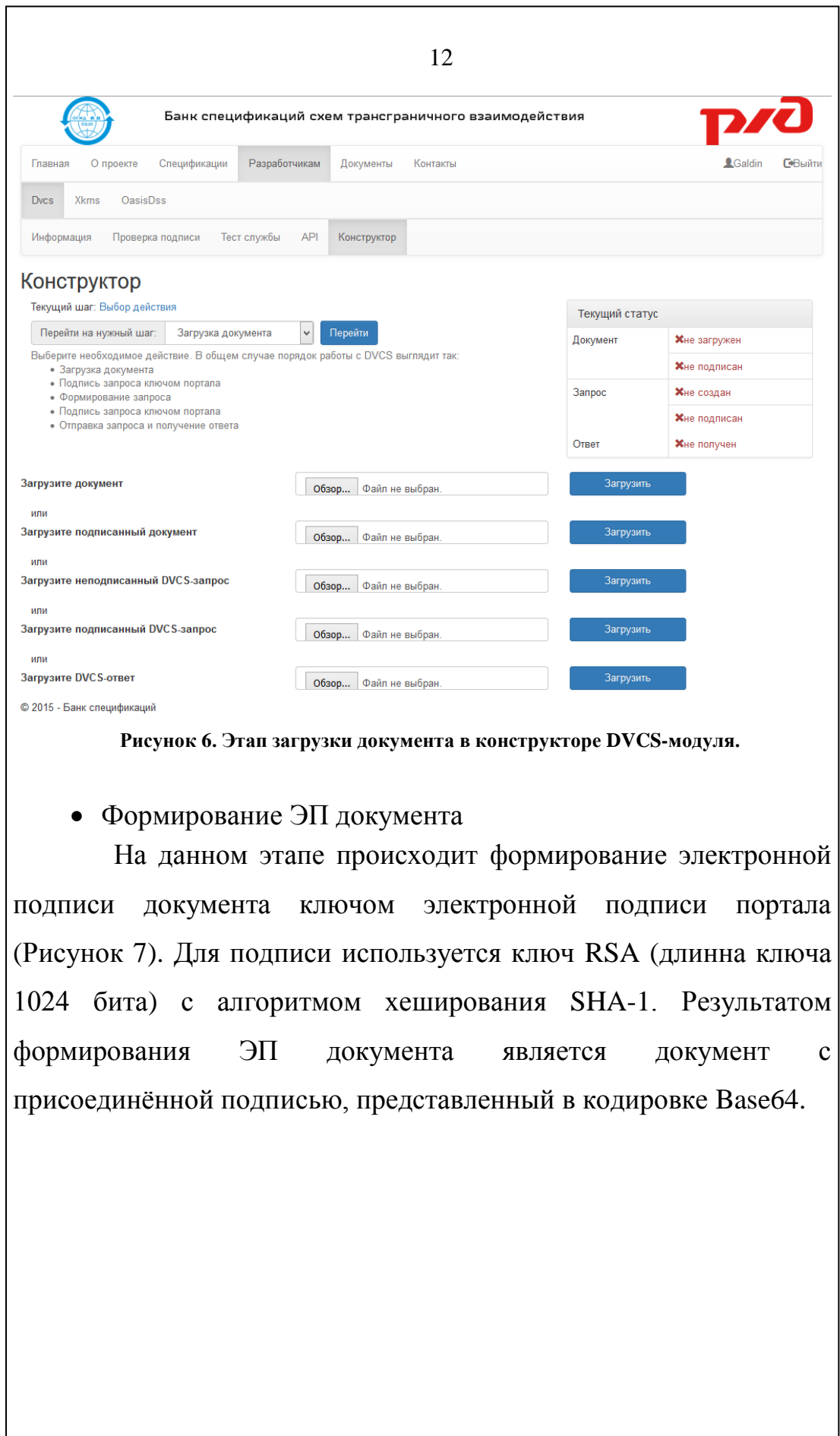


Рисунок 6. Этап загрузки документа в конструкторе DVCS-модуля.

- Формирование ЭП документа

На данном этапе происходит формирование электронной подписи документа ключом электронной подписи портала (Рисунок 7). Для подписи используется ключ RSA (длина ключа 1024 бита) с алгоритмом хеширования SHA-1. Результатом формирования ЭП документа является документ с присоединённой подписью, представленный в кодировке Base64.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

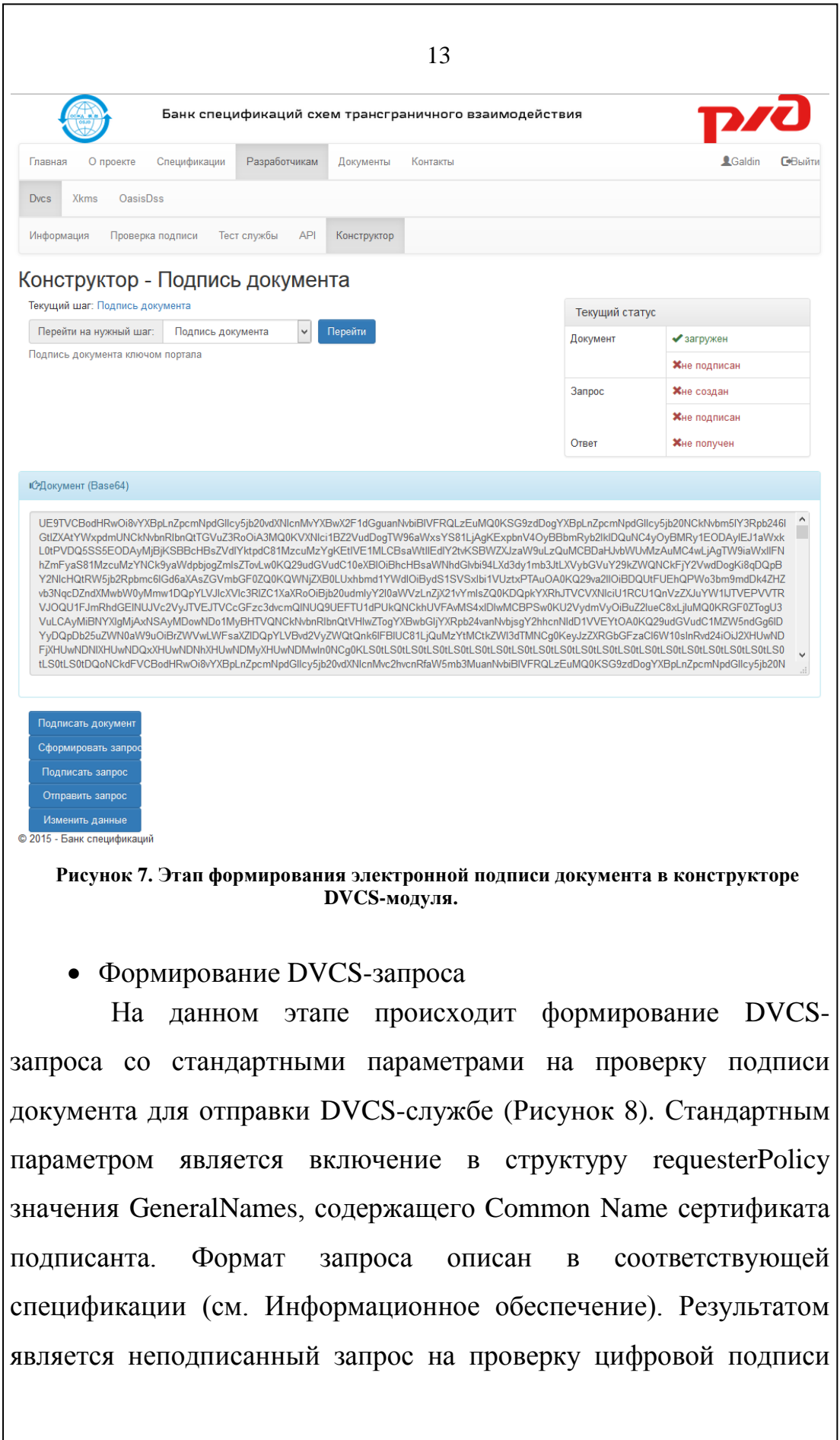


Рисунок 7. Этап формирования электронной подписи документа в конструкторе DVCS-модуля.

• Формирование DVCS-запроса

На данном этапе происходит формирование DVCS-запроса со стандартными параметрами на проверку подписи документа для отправки DVCS-службе (Рисунок 8). Стандартным параметром является включение в структуру requesterPolicy значения GeneralNames, содержащего Common Name сертификата подписанта. Формат запроса описан в соответствующей спецификации (см. Информационное обеспечение). Результатом является неподписанный запрос на проверку цифровой подписи

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лист	№	Подп.	Дата	Руководство пользователя	Лист

документа – Validation of Digitally Signed Document (VSD) DVCS-запрос, возвращаемый пользователю в кодировке Base64.

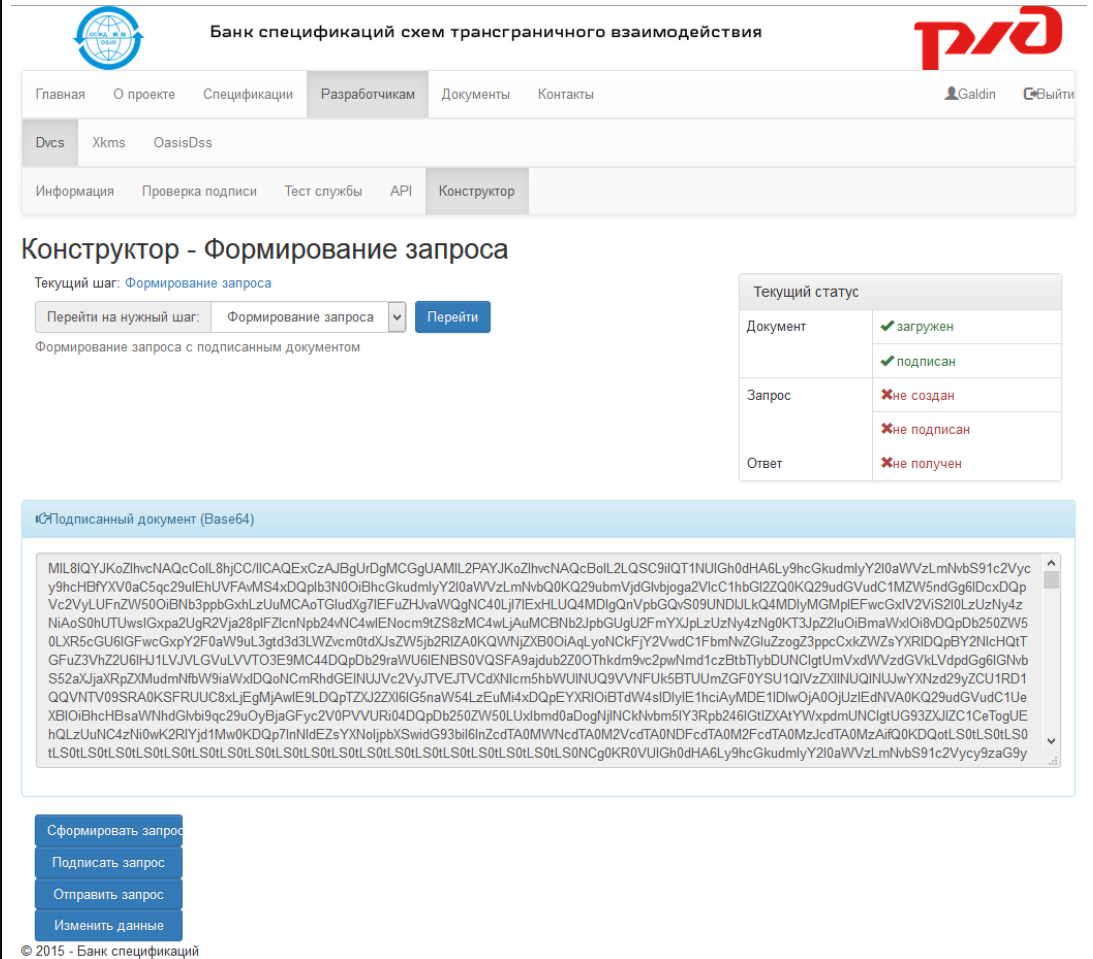


Рисунок 8. Этап формирования DVCS-запроса в конструкторе DVCS-модуля.

• Формирование ЭП DVCS-запроса

На данном этапе происходит формирование электронной подписи DVCS-запроса ключом электронной подписи портала (Рисунок 9). Для подписи используется ключ RSA (длина ключа 1024 бита) с алгоритмом хеширования SHA-1. Кроме того, ключ имеет необходимый для работы по протоколам DVCS идентификатор – «1.3.6.1.5.5.7.3.10». Результатом формирования

Ив.№ подл.	Подп. и дата	Ив.№ дубл.	Подп. и дата
Взам. инв. №			
Ив.№ подл.			

Лис	№	Подп.	Дата	Руководство пользователя	Лист
					14

ЭП DVCS-запроса является подписанный DVCS-запрос, представленный в кодировке Base64.

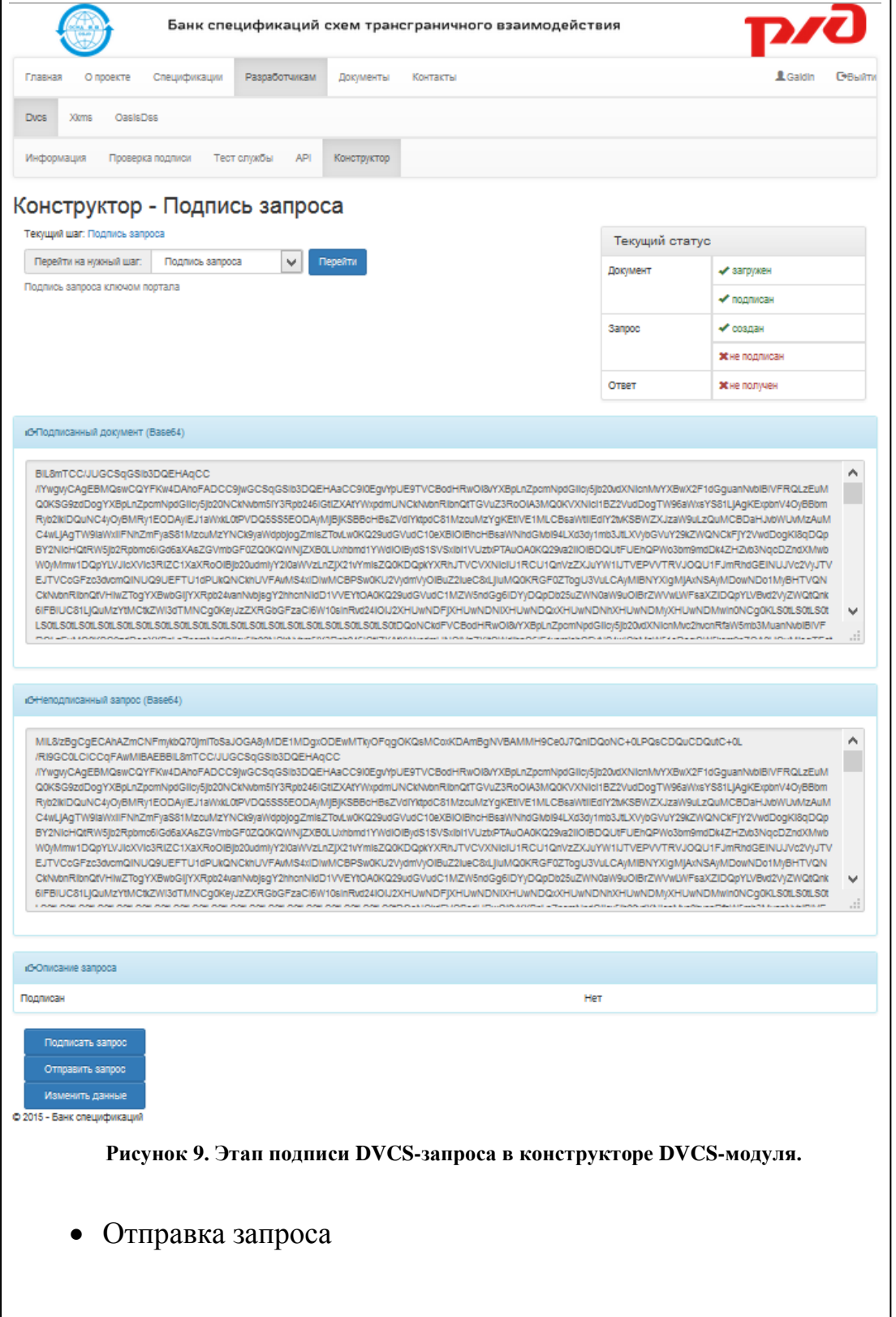


Рисунок 9. Этап подписи DVCS-запроса в конструкторе DVCS-модуля.

- Отправка запроса

Инв. № подл.	Подп. и дата
Взам. инв. №	Инв. № дубл.
Подп. и дата	Подп. и дата

Лис	№	Подп.	Дата	Руководство пользователя	Лист
					15

На данном этапе происходит отправка подписанного DVCS-запроса DVCS-службе и получение ответа (). Результатом является ответ на запрос в кодировке Base64.

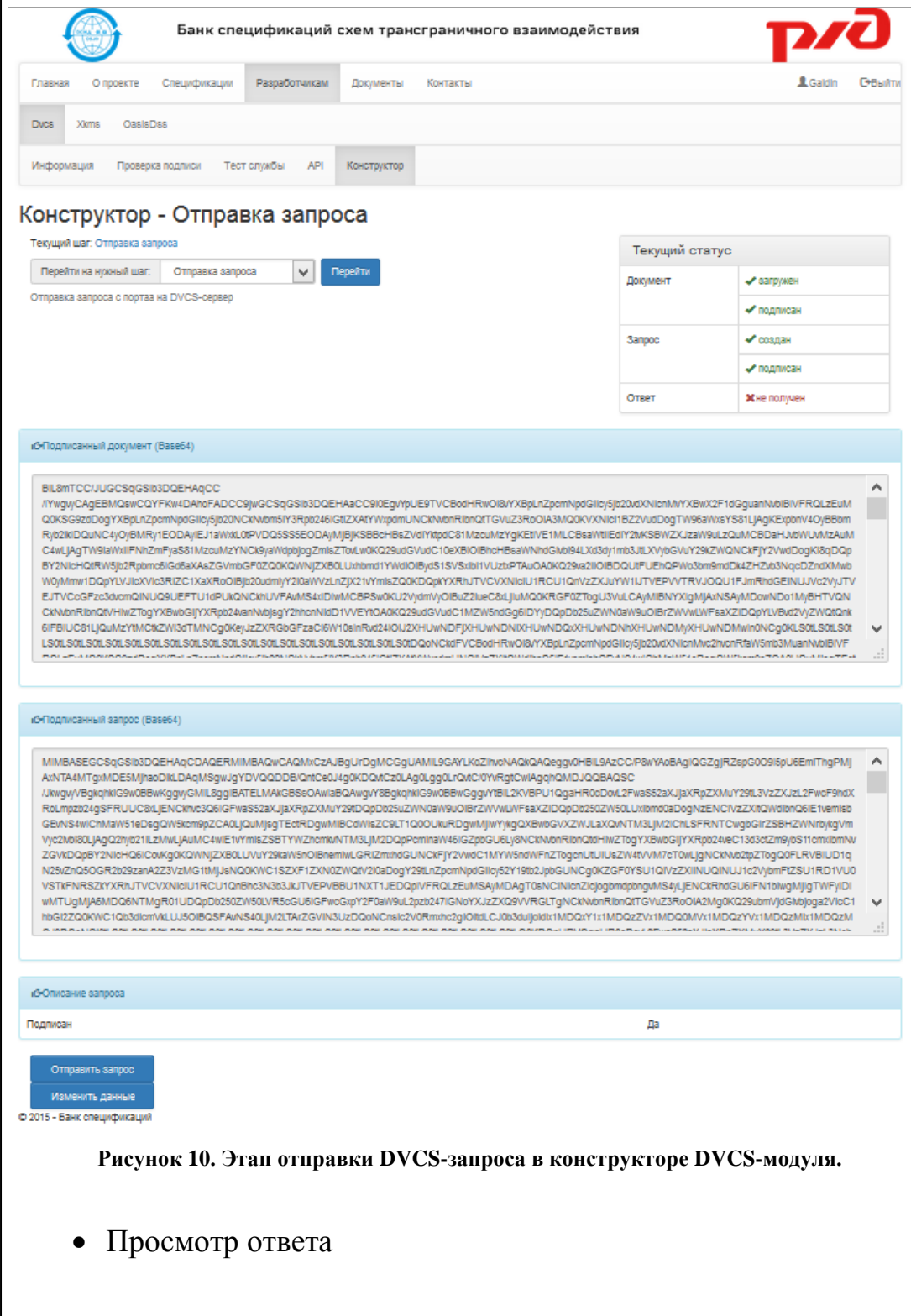


Рисунок 10. Этап отправки DVCS-запроса в конструкторе DVCS-модуля.

- Просмотр ответа

Инв. № подл.	Подп. и дата	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	Руководство пользователя	Лист
					16

На данном этапе происходит вывод ответа службы пользователю вместе с подписанным документом и подписанным DVCS-запросом (Рисунок 11).

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

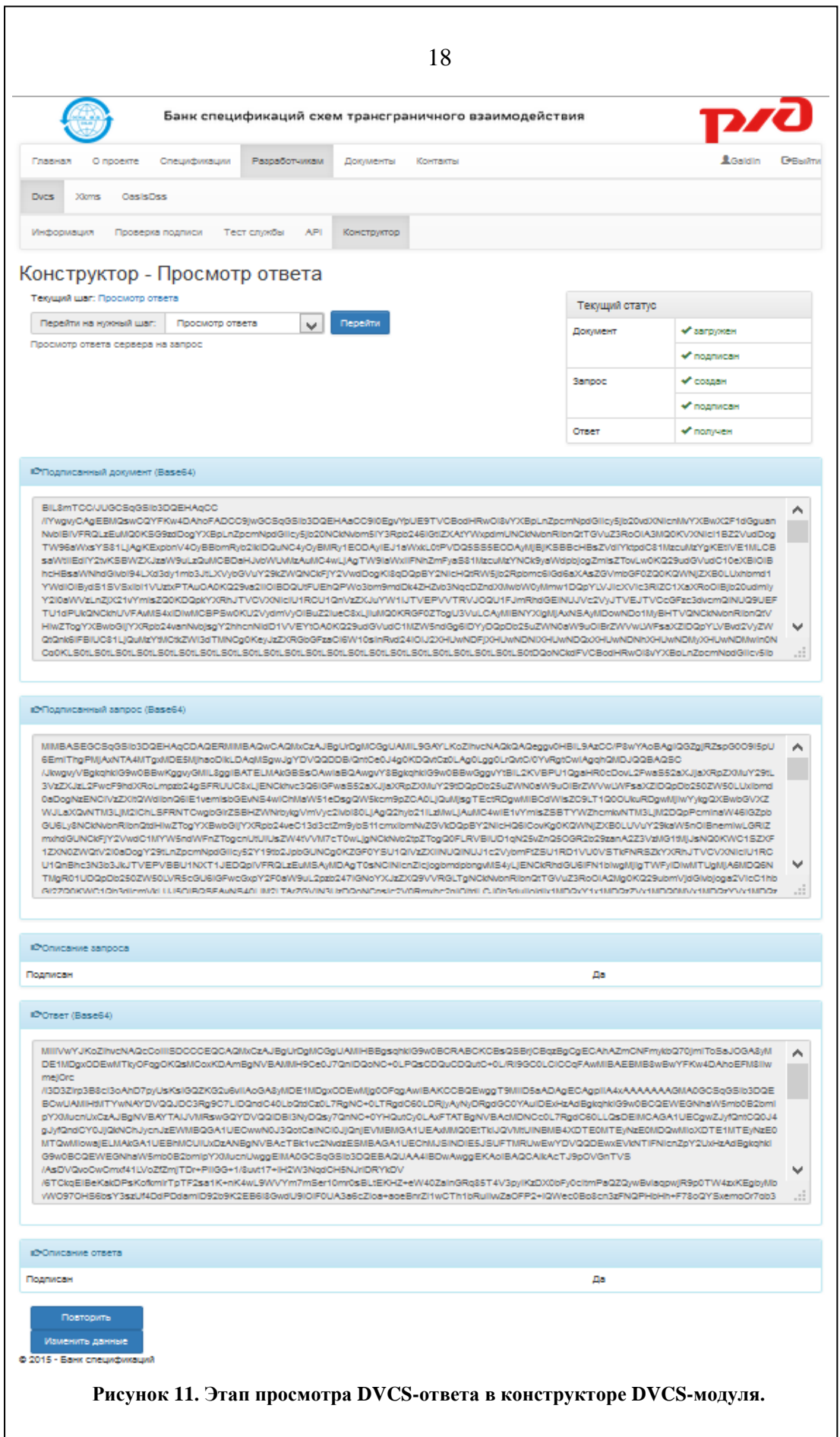


Рисунок 11. Этап просмотра DVCS-ответа в конструкторе DVCS-модуля.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

4. Работа с XKMS-модулем

ХКMS-модуль осуществляет взаимодействие с ХКMS-службой ДТС ОАО «РЖД»

Работа с ХКMS-модулем начинается на главной странице раздела «ХКMS».

Страницы «Информация» и «API» носят информационный характер и не взаимодействуют с ХКMS-модулем.

Страница «Проверка» позволяет проверить сертификат ключа электронной подписи через ХКMS-службу (Рисунок 12).

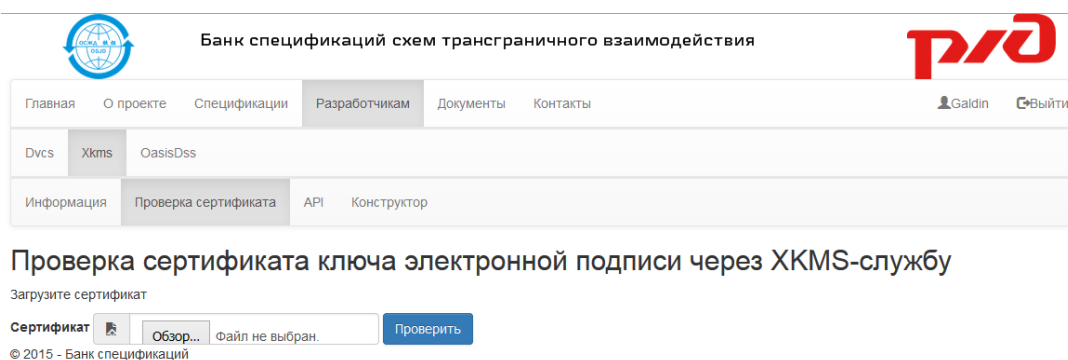


Рисунок 12. Страница проверки сертификата ключа электронной подписи через ХКMS-службу.

Для этого необходимо загрузить подписанный документ и нажать на кнопку «проверить». После этого будет сформирован и отправлен запрос на проверку, получен ответ и выведен результат. В случае, если проверка прошла успешно, будет выведена информация об успешной проверке, информация о загруженном файле и информация об ответе службы. В случае неудачи будет выведено сообщение об ошибке.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
Лис	№	Подп.	Дата	19		

Страница «Конструктор» позволяет наглядно ознакомиться и пройти по ключевым этапам взаимодействия по протоколу XKMS:

- **Загрузка сертификата**

На данном этапе происходит загрузка сертификата ключа электронной подписи, который будет проверен. Можно загрузить сформированный подписанный/не подписанный запрос или ответ и сразу перейти к нужному шагу (Рисунок 13). Результатом является информация о сертификате ключа ЭП.

Рисунок 13. Этап загрузки сертификата ключа проверки электронной подписи в конструкторе XKMS-модуля.

- **Формирование XKMS-запроса**

На данном этапе происходит формирование XKMS-запроса со стандартными параметрами на проверку подписи документа для отправки DVCS-службе (Рисунок 14). Стандартным

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

Лис	№	Подп.	Дата

параметром является включение элемента <RespondWith> со значением X509CRL (<http://www.w3.org/2002/03/xkms#X509CRL>) – указанием на возврат информации о проверке по спискам отзыва сертификатов в XKMS-ответе. Формат запроса описан в соответствующей спецификации (см. Информационное обеспечение). Результатом является неподписанный запрос на проверку сертификата ключа ЭП к службе информации о ключах – X-KISS Validate Service XKMS-запрос, возвращаемый пользователю в XML.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	Руководство пользователя					Лист
										21
	Лис	№	Подп.	Дата						

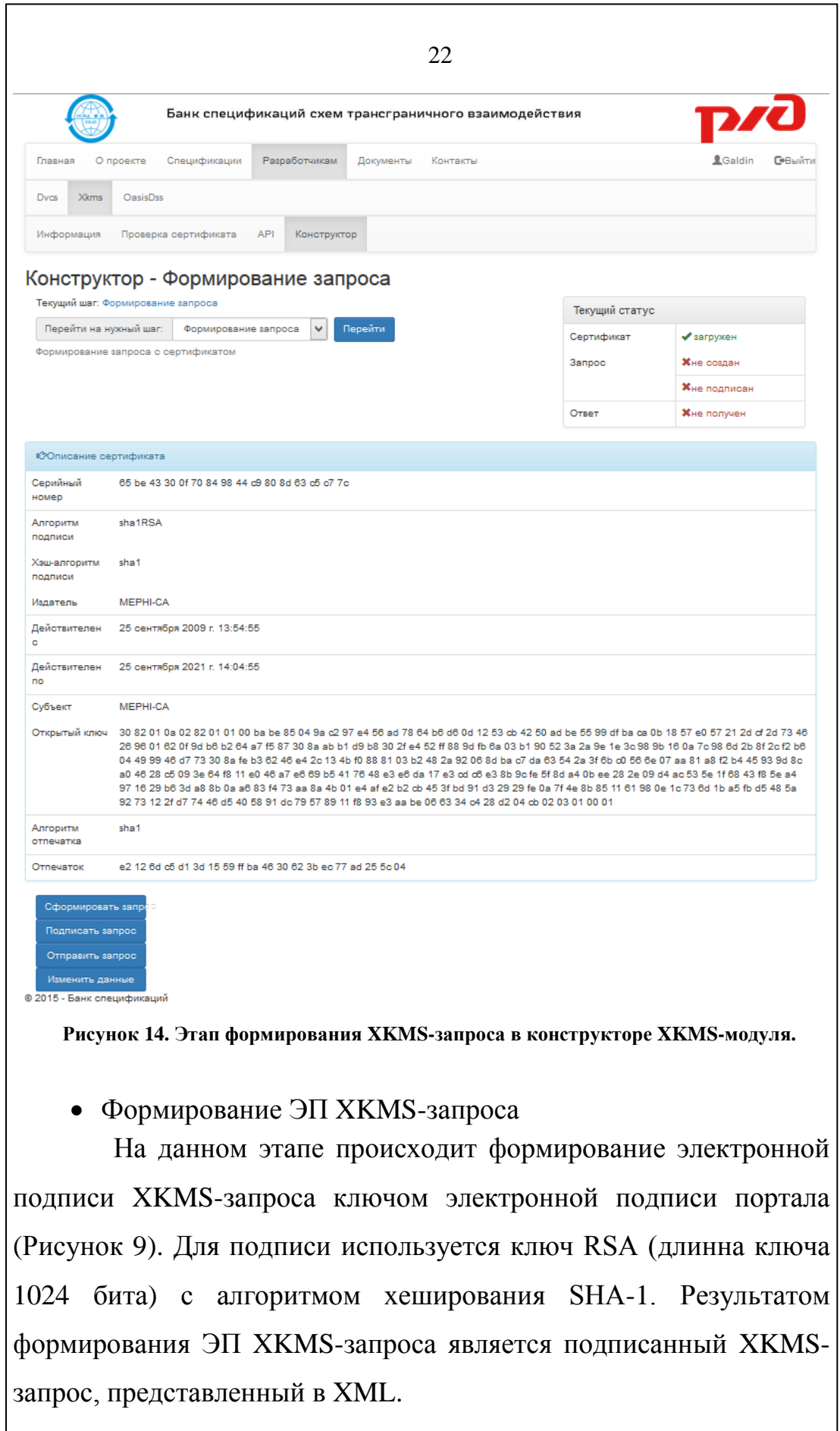


Рисунок 14. Этап формирования XKMS-запроса в конструкторе XKMS-модуля.

- Формирование ЭП XKMS-запроса

На данном этапе происходит формирование электронной подписи XKMS-запроса ключом электронной подписи портала (Рисунок 9). Для подписи используется ключ RSA (длина ключа 1024 бита) с алгоритмом хеширования SHA-1. Результатом формирования ЭП XKMS-запроса является подписанный XKMS-запрос, представленный в XML.

Инд. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	Руководство пользователя	Лист
					22

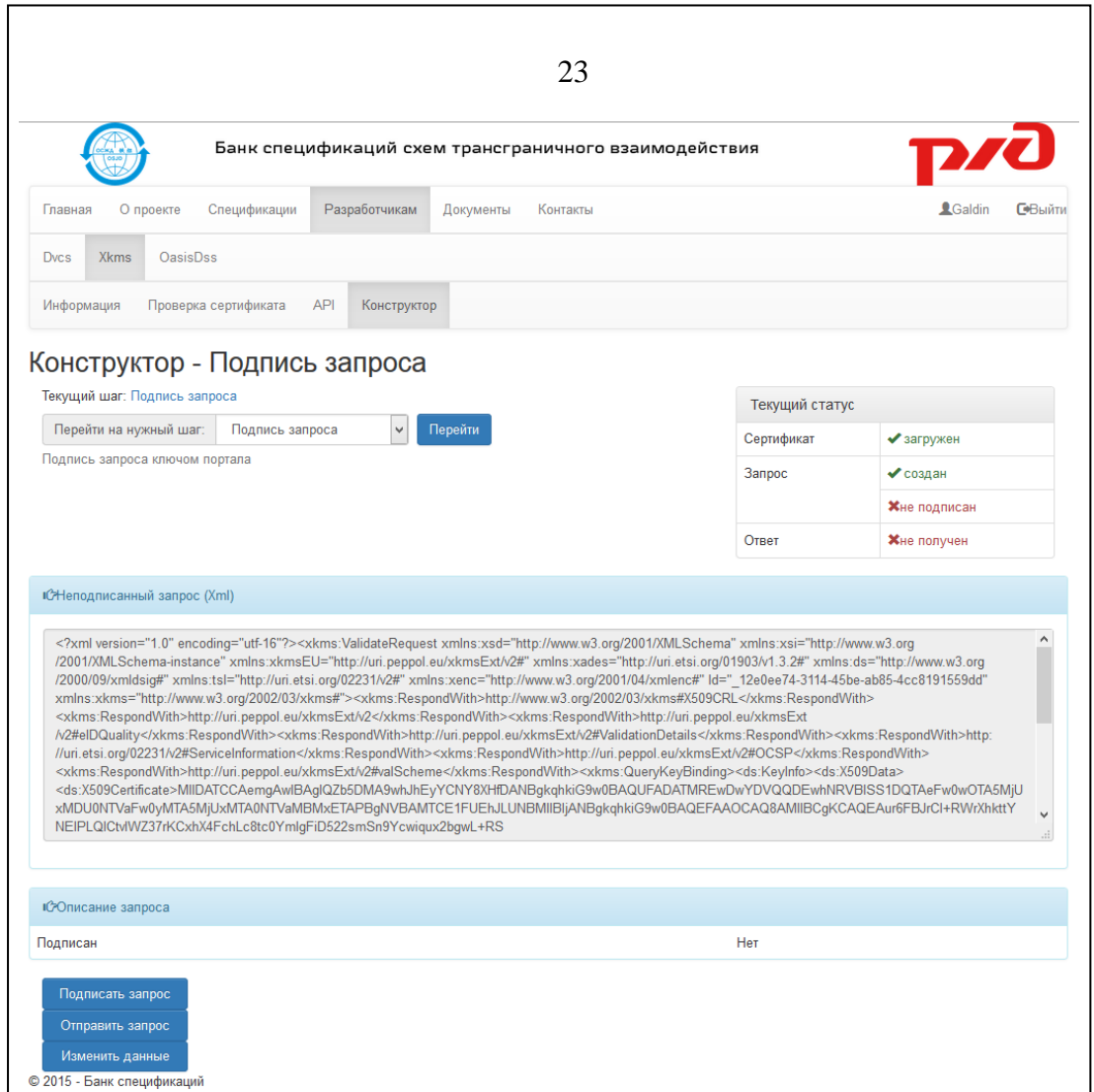


Рисунок 15. Этап подписи XKMS-запроса в конструкторе XKMS-модуля.

- Отправка запроса

На данном этапе происходит отправка подписанного XKMS-запроса XKMS-службе и получение ответа (Рисунок 16). Результатом является ответ на запрос в XML.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

Банк спецификаций схем трансграничного взаимодействия

Главная О проекте Спецификации Разработчикам Документы Контакты

Dvcs Xkms OasisDss

Информация Проверка сертификата API Конструктор

Конструктор - Отправка запроса

Текущий шаг: **Отправка запроса**

Перейти на нужный шаг: Отправка запроса

Отправка запроса с порта на XKMS-сервер

Текущий статус	
Сертификат	✓ загружен
Запрос	✓ создан
	✓ подписан
Ответ	✗ не получен

Подписанный запрос (xml)

```
<xkms:ValidateRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xkmsEU="http://uri.peppol.eu/xkmsExt/v2#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
xmlns:tsl="http://uri.etsi.org/02231/v2#" xmlns:xenc="http://www.w3.org/2001/04/xmenc#" Id="_37b9ba73-ef46-4ba4-a7b2-0a3d86f7110"
xmlns:xkms="http://www.w3.org/2002/03/xkms#"><ds:Signature id="XMLSignature_v.1.0"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><ds:Reference
URI="#_37b9ba73-ef46-4ba4-a7b2-0a3d86f7110"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09
/xmldsig#sha1" /><ds:DigestValue>aFY0Phe1sPLiw3tMeoobUxN6qcg=</ds:DigestValue></ds:Reference></ds:SignedInfo>
<ds:SignatureValue>MS0Bc2E9KugDbGuVvVcxONL0AjDbxUexcwim6Wibw1qcjXVDpiHas4156jg9Cj1wzKO2NB0/kdTOBZzFzjjob7n0V+wBW/xlbwAJ7MBAF
/qfmcGuXUtxKi6dxiBi/rkgGifSOd6dAQAAfVYh/qu7S+cJhmWfVf1x/gMunSH6I=</ds:SignatureValue><ds:KeyInfo><ds:X509Data>
<ds:X509Certificate>MIIHTCCA4agAwIBAgIQALamHNtd09IEgmnzJ0mzANBgkqhkiG9w0BAQUFADCCAUsxCzAJBgNVBAYTAUVMRgwFgYDVQQLDA83NyDQn
```

Описание запроса

Подписан Да

© 2015 - Банк спецификаций

Рисунок 16. Этап отправки XKMS-запроса в конструкторе XKMS-модуля.

• Просмотр ответа

На данном этапе происходит вывод ответа службы пользователю вместе с подписанным XKMS-запросом ().

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
Лис	№	Подп.	Дата			

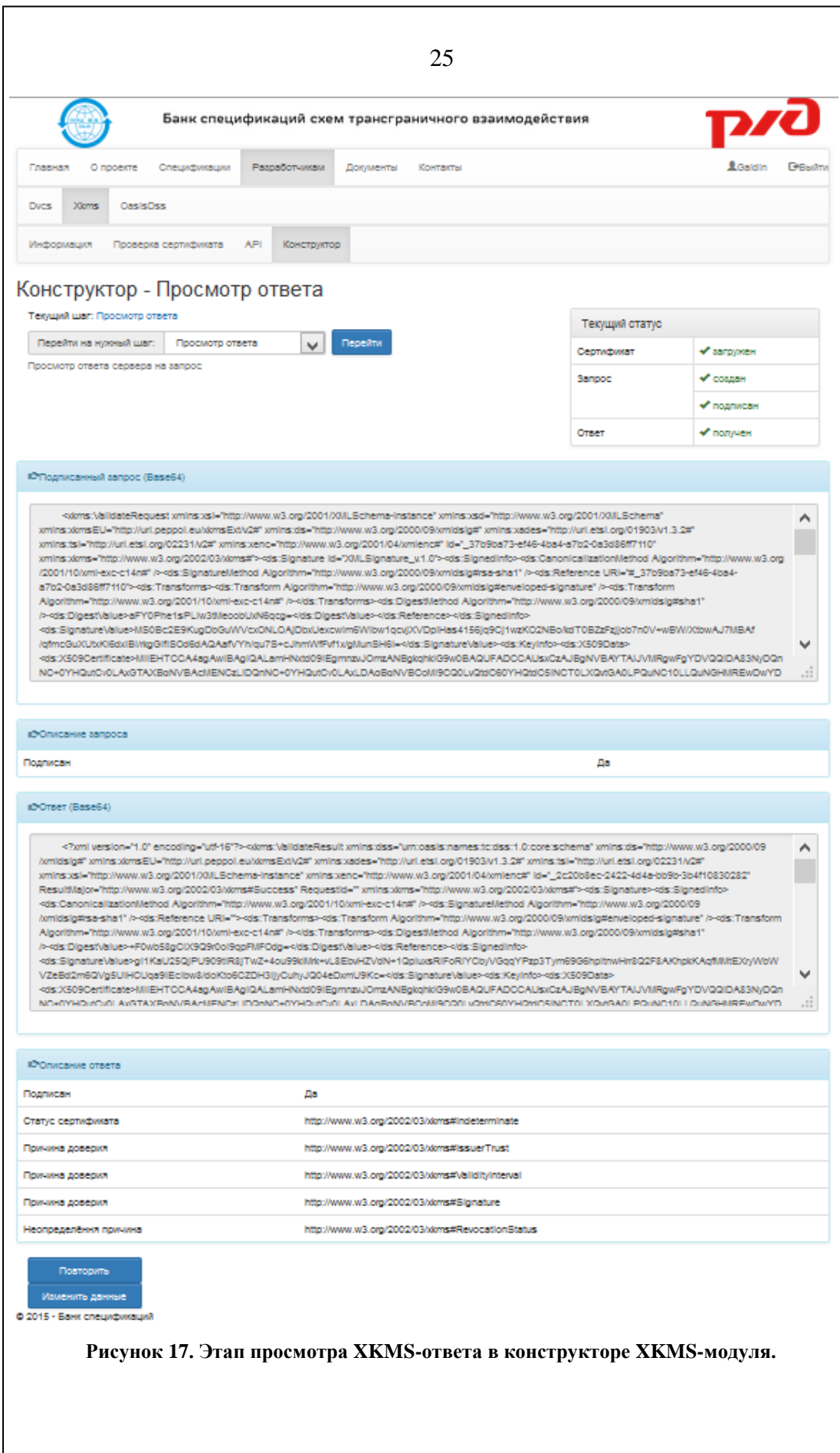


Рисунок 17. Этап просмотра XKMS-ответа в конструкторе XKMS-модуля.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	

Лис	№	Подп.	Дата
-----	---	-------	------

5. Работа с OASIS DSS-модулем

OASIS DSS-модуль осуществляет взаимодействие с OASIS DSS-службой ДТС ОАО «РЖД»

Работа с OASIS DSS-модулем начинается на главной странице раздела «OASIS DSS».

Страницы «Информация» и «API» носят информационный характер и не взаимодействуют с OASIS DSS-модулем.

Страница «Проверка» позволяет проверить присоединённую подпись документа через OASIS DSS-службу.

Для этого необходимо загрузить подписанный документ и нажать на кнопку «проверить». После этого будет сформирован и отправлен запрос на проверку, получен ответ и выведен результат. В случае, если проверка прошла успешно, будет выведена информация об успешной проверке, информация о загруженном файле и информация об ответе службы. В случае неудачи будет выведено сообщение об ошибке.

Страница «Конструктор» позволяет наглядно ознакомиться и пройти по ключевым этапам взаимодействия по протоколу OASIS DSS:

- Загрузка документа

На данном этапе происходит загрузка документа, который в дальнейшем будет подписан и подпись которого будет проверена. Можно загрузить подписанный документ,

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

					Руководство пользователя	Лист
	Лис	№	Подп.	Дата		26

сформированный подписанный/не подписанный запрос или ответ и сразу перейти к нужному шагу.

- **Формирование ЭП документа**

На данном этапе происходит формирование электронной подписи документа ключом электронной подписи портала. Для подписи используется ключ RSA (длина ключа 1024 бита) с алгоритмом хеширования SHA-1. Результатом формирования ЭП документа является документ с присоединённой подписью, представленный в XML.

- **Формирование OASIS DSS-запроса**

На данном этапе происходит формирование OASIS DSS-запроса со стандартными параметрами на проверку подписи документа для отправки OASIS DSS-службе. Формат запроса описан в соответствующей спецификации (см. Информационное обеспечение). Результатом является неподписанный запрос на проверку цифровой подписи документа – OASIS DSS Verify Request, возвращаемый пользователю в XML.

- **Формирование ЭП OASIS DSS-запроса**

На данном этапе происходит формирование электронной подписи OASIS DSS-запроса ключом электронной подписи портала. Для подписи используется ключ RSA (длина ключа 1024 бита) с алгоритмом хеширования SHA-1. Результатом формирования ЭП OASIS DSS-запроса является подписанный OASIS DSS-запрос, представленный в XML.

- **Отправка запроса**

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

На данном этапе происходит отправка подписанного OASIS DSS-запроса OASIS DSS-службе и получение ответа. Результатом является ответ на запрос в XML.

- **Просмотр ответа**

На данном этапе происходит вывод ответа службы пользователю вместе с подписанным документом и подписанным OASIS DSS-запросом.

6. Тестирование внешней службы

Тестирование внешней VSD-службы производится на странице «Тест службы» подраздела «DVCS» раздела «Разработчикам» Портала (Рисунок 18).

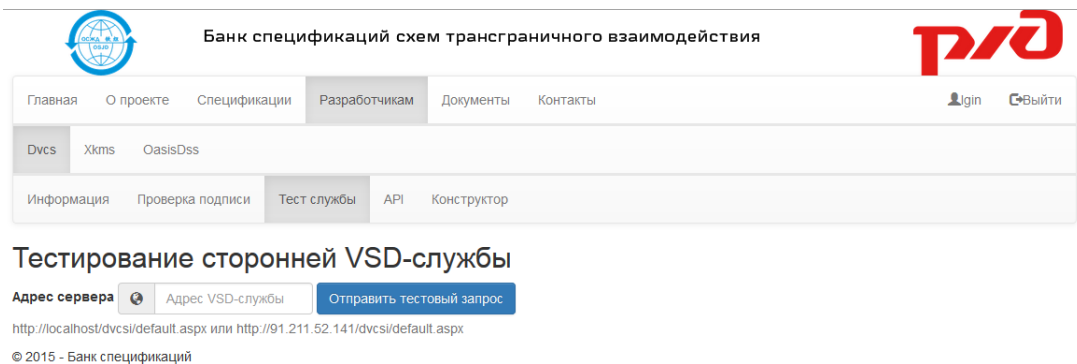


Рисунок 18. Страница тестирования внешней VSD DVCS-службы.

При тестировании внешней VSD-службы производится проверка готовности принимать и обрабатывать запросы и предоставлять правильные ответы на них. Проверка производится путём формирования и отправки тестового запроса. В случае, если

Инв. № подл.	Подп. и дата
Взам. инв. №	Инв. № дубл.
Подп. и дата	Подп. и дата

					Руководство пользователя	Лист
Лис	№	Подп.	Дата			28

служба смогла обработать запрос, то будет выведена информация о полученном ответе (Рисунок 19).

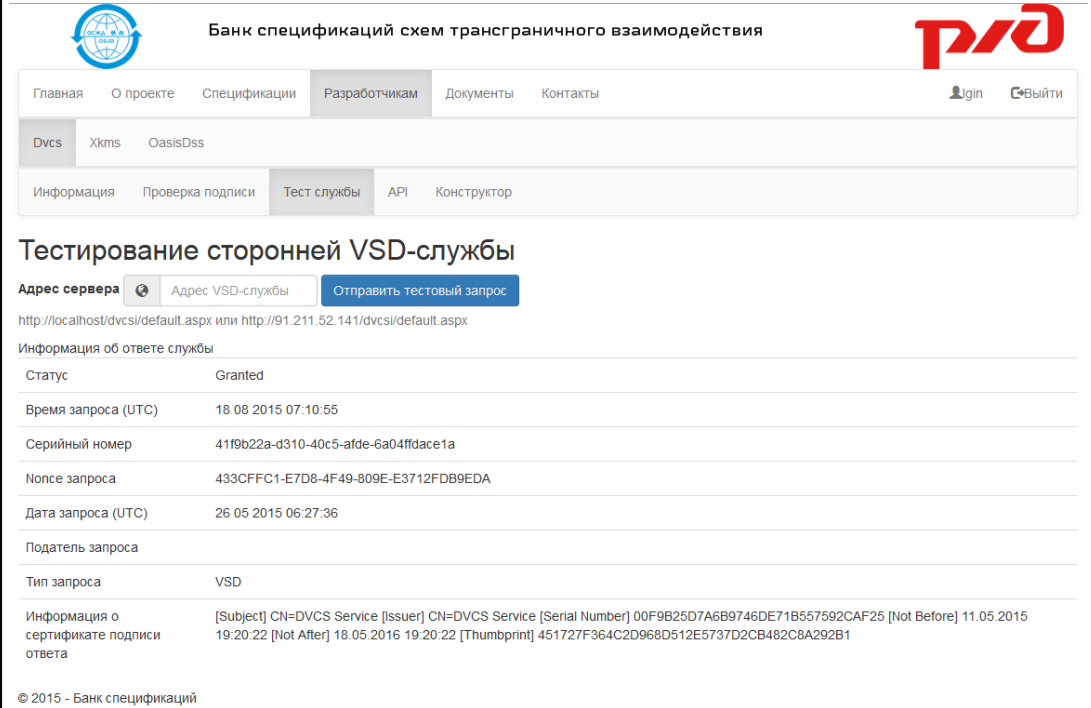


Рисунок 19. Результат тестирования внешней VSD DVCS-службы.

Вероятнее всего для обеспечения правильной обработки запроса с портала потребуется разрешить обработку сертификатов ключей ЭП, которыми подписываются документы и запросы на портале (добавить их в список доверенных).

Сам портал при тестировании сторонней службы проверяет у ответа лишь математическую корректность подписи.

7. Прикладой программный интерфейс

Прикладной программный интерфейс (application programming interface, API) – набор готовых классов, процедур,

Ивв. № подл.	Подп. и дата	Взам. инв. №	Ивв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	Руководство пользователя	Лист
					29

функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах.

API Портала банка спецификаций предоставляет доступ по протоколу SOAP к основным операциям в каждом из программных модулей через службы DvcsService, XkmsService и OasisDssService.

Методы возвращают один из двух типов объектов – BinaryResult или StringResult. Разница между ними лишь в типе поля data.

Класс BinaryResult:

```
public class BinaryResult
{
    public bool isOk;
    public byte[] data;
    public string error;
}
```

Класс StringResult:

```
public class StringResult
{
    public bool isOk;
    public string data;
    public string error;
}
```

isOk – флаг; true, если метод завершился успешно (без ошибок), false в противном случае;

data – возвращаемые методом данные;

error – поле для записи информации об ошибке.

7.1. DvcsService предоставляет методы:

- *BinaryResult* SignDoc(byte[] document)

Подпись документа ключом ЭП Портала.

document – документ для подписи.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лист	№	Подп.	Дата	

BinaryResult – возвращаемый объект, содержащий подписанный документ.

- *BinaryResult* CreateRequest(byte[] *signedDocument*)

Формирование DVCS-запроса

signedDocument – подписанный документ.

BinaryResult – возвращаемый объект, содержащий неподписанный запрос.

- *BinaryResult* SignRequest(byte[] *request*)

Формирование ЭП DVCS-запроса.

request – неподписанный запрос.

BinaryResult – возвращаемый объект, содержащий подписанный запрос.

- *BinaryResult* SendRequest(byte[] *signedRequest*)

Отправка запроса.

signedRequest – подписанный запрос.

BinaryResult – возвращаемый объект, содержащий ответ.

7.2. XkmsService предоставляет методы:

- *StringResult* CreateRequest(byte[] *X509Certificate*)

Формирование XKMS-запроса

X509Certificate – сертификат на проверку.

StringResult – возвращаемый объект, содержащий неподписанный запрос.

- *StringResult* SignRequest(string *request*)

Формирование ЭП XKMS-запроса.

request – неподписанный запрос.

StringResult – возвращаемый объект, содержащий подписанный запрос.

- *StringResult* SendRequest(string *signedRequest*)

Отправка запроса.

signedRequest – подписанный запрос.

StringResult – возвращаемый объект, содержащий ответ.

7.3. OasisDssService предоставляет методы:

- *BinaryResult* SignDoc(byte[] *document*)

Интв. № подл.	Подп. и дата	Взам. инв. №	Интв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	

Подпись документа ключом ЭП Портала.

document – документ для подписи.

BinaryResult – возвращаемый объект, содержащий подписанный документ.

- *StringResult CreateRequest(byte[] signedDocument)*

Формирование OASIS DSS-запроса

signedDocument – подписанный документ.

StringResult – возвращаемый объект, содержащий неподписанный запрос.

- *StringResult SignRequest(byte[] request)*

Формирование ЭП OASIS DSS-запроса.

request – неподписанный запрос.

StringResult – возвращаемый объект, содержащий подписанный запрос.

- *StringResult SendRequest(byte[] signedRequest)*

Отправка запроса.

signedRequest – подписанный запрос.

StringResult – возвращаемый объект, содержащий ответ.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Лис	№	Подп.	Дата	