

УТВЕРЖДАЮ

Генеральный директор

ООО «Кейсистемс»

_____ А. А. Матросов

«__» _____ 2019 г.

ПРОГРАММНЫЙ КОМПЛЕКС «ПРОЕКТ–СМАРТ ПРО»
Версия 18.0

Руководство пользователя

Настройка SSL на IIS

ЛИСТ УТВЕРЖДЕНИЯ

Инв. N подл	Подп и дата
Взам. инв. N	Подп и дата
Инв. N дубл	Подп и дата

СОГЛАСОВАНО

Заместитель генерального директора

ООО «Кейсистемс»

_____ О. С. Семенов

«__» _____ 2019 г.

Руководитель ДПиАБ

_____ А. В. Никитин

«__» _____ 2019 г.

2019

Литера А

УТВЕРЖДЕНО



ПРОГРАММНЫЙ КОМПЛЕКС «ПРОЕКТ–СМАРТ ПРО» ВЕРСИЯ 18.0

Руководство пользователя

Настройка SSL на IIS

Листов 17

Инв. N подл	Подп и дата	Взам. инв. N	Инв. N дубл	Подп и дата

2019

Литера А

АННОТАЦИЯ

Настоящий документ является частью руководства администратора программного комплекса «Проект-смарт ПРО» версии 18.0 и содержит описание операций по созданию и настройке сертификатов SSL на IIS в ОС «WINDOWS».

Руководство актуально для указанной версии и для последующих версий вплоть до выпуска обновления руководства.

Порядок выпуска обновлений руководства

Выход новой версии программного комплекса сопровождается обновлением руководства только в случае наличия в версии значительных изменений режимов, описанных в руководстве, добавления новых режимов или изменения общей схемы работы. Если таких изменений версия не содержит, то остается актуальным руководство пользователя от предыдущей версии с учетом изменений, содержащихся в новой версии.

Перечень изменений версии программного комплекса содержится в сопроводительных документах к версии. Информация об изменениях руководства пользователя публикуется на сайте разработчика в разделе «Документация».

Информация о разработчике ПК «Проект–Смарт ПРО»

ООО «Кейсистемс»

Адрес: 428000, Чебоксары, Главпочтамт, а/я 172

Телефон: (8352) 323-323

Факс: (8352) 571-033

<http://www.keysystems.ru>

E-mail: info@keysystems.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1. НАСТРОЙКА SSL НА ПС.....	5
1.1. Сертификаты для настройки HTTPS сайта на ПС	5
1.2. Генерация CSR запроса на ПС 7.....	6
1.2.1. Создание запроса сертификата	7
1.2.2. Создание самозаверенного сертификата	10
1.3. Установка SSL в PFX.....	12
ГЛОССАРИЙ.....	15
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	16
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	17

ВВЕДЕНИЕ

Настоящее руководство содержит описание операций по установке web-сервисов для работы программного комплекса на ОС «WINDOWS».





Уровень подготовки пользователя

Для успешного освоения материала, изложенного в руководстве, и формирования навыков работы в программном комплексе с описанными режимами к пользователю предъявляются следующие требования:

- наличие опыта работы с персональным компьютером на базе операционных систем Windows на уровне квалифицированного пользователя;
- умение свободно осуществлять базовые операции в стандартных приложениях Windows.

словные обозначения

В документе используются следующие условные обозначения:

	Уведомление	–	Важные сведения о влиянии текущих действий пользователя на выполнение других функций, задач программного комплекса.
	Предупреждение	–	Важные сведения о возможных негативных последствиях действий пользователя.
	Предостережение	–	Критически важные сведения, пренебрежение которыми может привести к ошибкам.
	Замечание	–	Полезные дополнительные сведения, советы, общеизвестные факты и выводы.
[Выполнить]		–	Функциональные экранные кнопки.
<F1>		–	Клавиши клавиатуры.
«Чек»		–	Наименования объектов обработки (режимов).
Статус		–	Названия элементов пользовательского интерфейса.
ОКНА => НАВИГАТОР		–	Навигация по пунктам меню и режимам.
n. 2.1.1		–	Ссылки на структурные элементы, рисунки, таблицы текущего документа.
рисунок 5		–	Ссылки на документы из перечня ссылочных документов.
[1]		–	

1. НАСТРОЙКА SSL НА IIS

Подключение к базе данных может осуществляться как напрямую, так и с использованием сервера приложений. Выбор варианта подключения осуществляется в окне авторизации пользователей на вкладке «Соединение» (Рисунок 1).

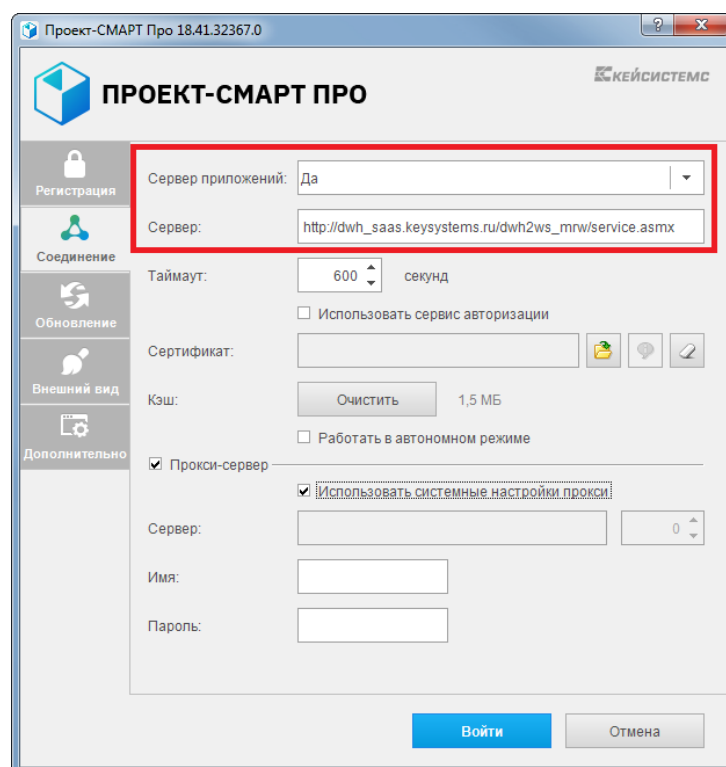


Рисунок 1. Вкладка «Соединение»

При использовании сервера приложений необходимо выбрать в поле **Сервер приложений** опцию «Да» и ввести адрес сервера в поле **Сервер** окна настройки соединения.

Для подключения через сервер приложений рекомендуется использовать https сервер с SSL, т.е. расширение протокола http, поддерживающее шифрование.

Протокол SSL (Secure Sockets Layer – уровень защищенных сокетов) используется для защиты данных в сети Интернет. Он гарантирует безопасное соединение между компьютером пользователя и сервером. При использовании SSL-протокола информация передается в закодированном виде по https и расшифровать ее можно только с помощью специального ключа (в отличие от протокола http). Для работы SSL-протокола требуется, чтобы на сервере был установлен SSL-сертификат.

Для выполнения настройки SSL на Windows Server, начиная от 2008 R2 и выше, должен быть установлен веб сервер IIS.

1.1. Сертификаты для настройки https сайта на IIS

Чтобы подготовить веб-сервер для обработки HTTPS-соединений, администратор должен получить и установить в систему сертификат для этого веб-сервера. Сертификат состоит из двух частей (двух ключей) – public и private. Public-часть сертификата используется для шифрования трафика от клиента к серверу в защищенном соединении; private-часть – для расшифровывания полученного от клиента зашифрованного трафика на сервере.

Необходимо прописать все DNS записи и сгенерировать Certificate Signing Request (CSR) запрос - запрос на получение сертификата, который представляет собой текстовый файл, содержащий в закодированном виде информацию об администраторе домена и открытый ключ. CSR можно сгенерировать в процессе заказа SSL-сертификата или на стороне веб-сервера на выпуск сертификата. Задачей CSR является подготовка специального файла, в составе которого будет содержаться необходимая информация о домене, на который планируется выпустить SSL сертификат и информация об организации, всё это будет зашифровано. Вместе с CSR будет сгенерирован закрытый ключ (private key), которым сервер или сервис будет расшифровывать трафик между ним и клиентом (Рисунок 2).

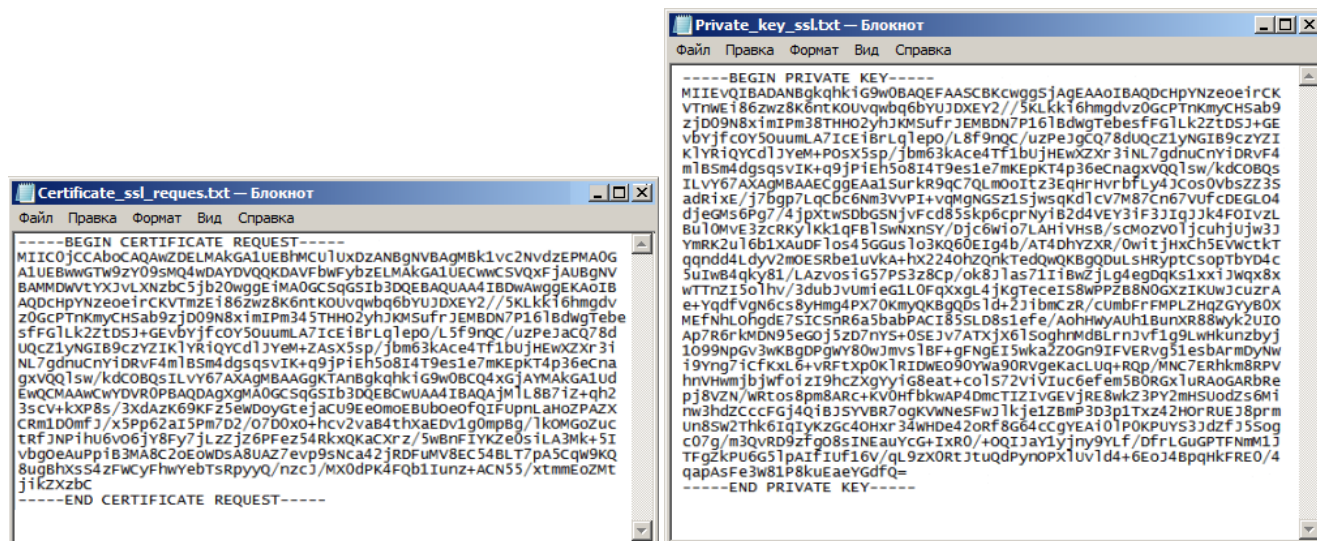


Рисунок 2. Запрос и закрытый ключ

После того как пара ключей приватный/публичный сгенерированы, на основе публичного ключа формируется запрос на SSL-сертификат в Центр сертификации (п. 1.2.1).

Существует возможность создать такой сертификат, не обращаясь в Центр сертификации. Подписываются такие сертификаты этим же сертификатом, поэтому они называются «самоподписанными»/«самозаверенными» (self-signed) (п. 1.2.2).



При отсутствии дополнительных рекомендаций и требований к сертификату, рекомендуется использование опции «Создать самозаверенный сертификат».

1.2. Генерация CSR запроса на IIS 7

Откройте консоль управления IIS. Для создания сайтов на протоколе https прежде всего необходимо создать и импортировать нужный сертификат. Для этого откройте диспетчер IIS и перейдите в пункт «Сертификаты сервера» (Рисунок 3).

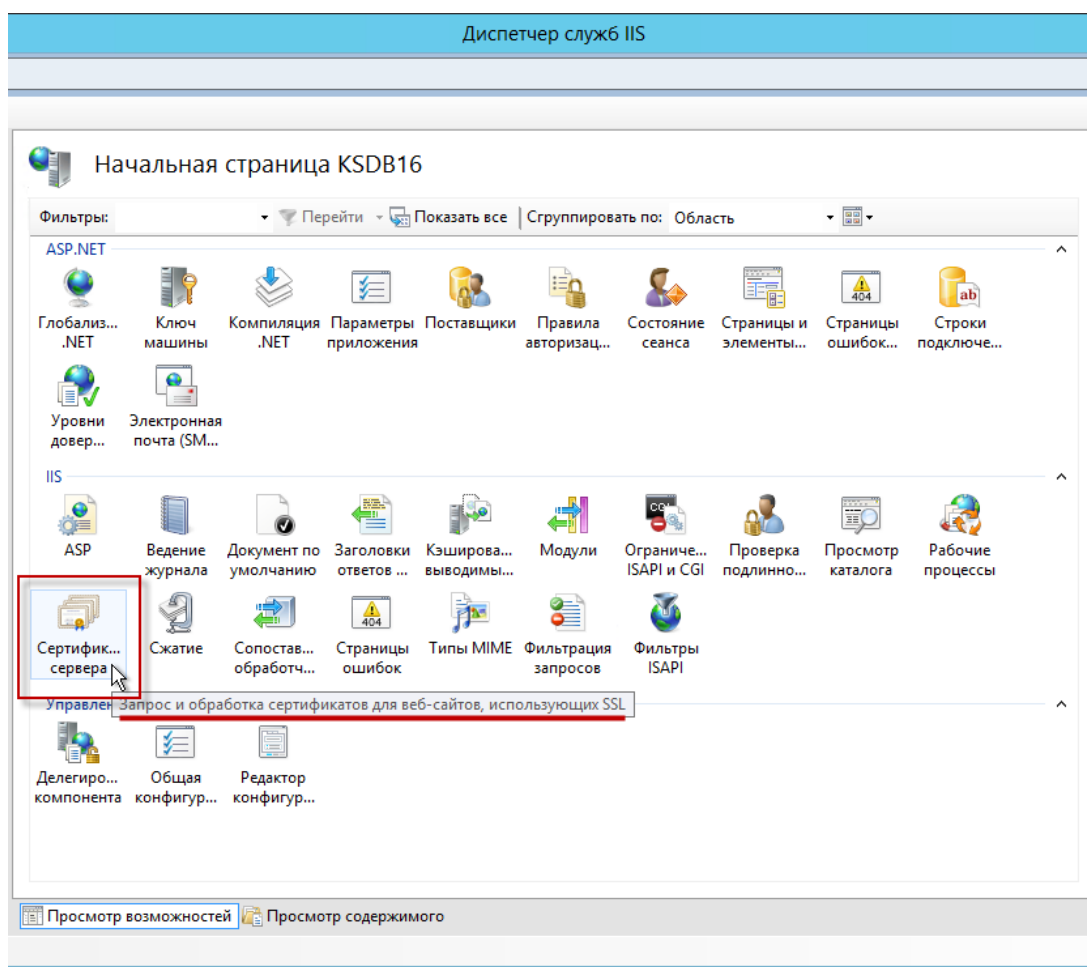


Рисунок 3. Сертификаты сервера

1.2.1. Создание запроса сертификата

В открывшемся окне, в области «Действия», выберите опцию «Создать запрос сертификата» (Рисунок 4).

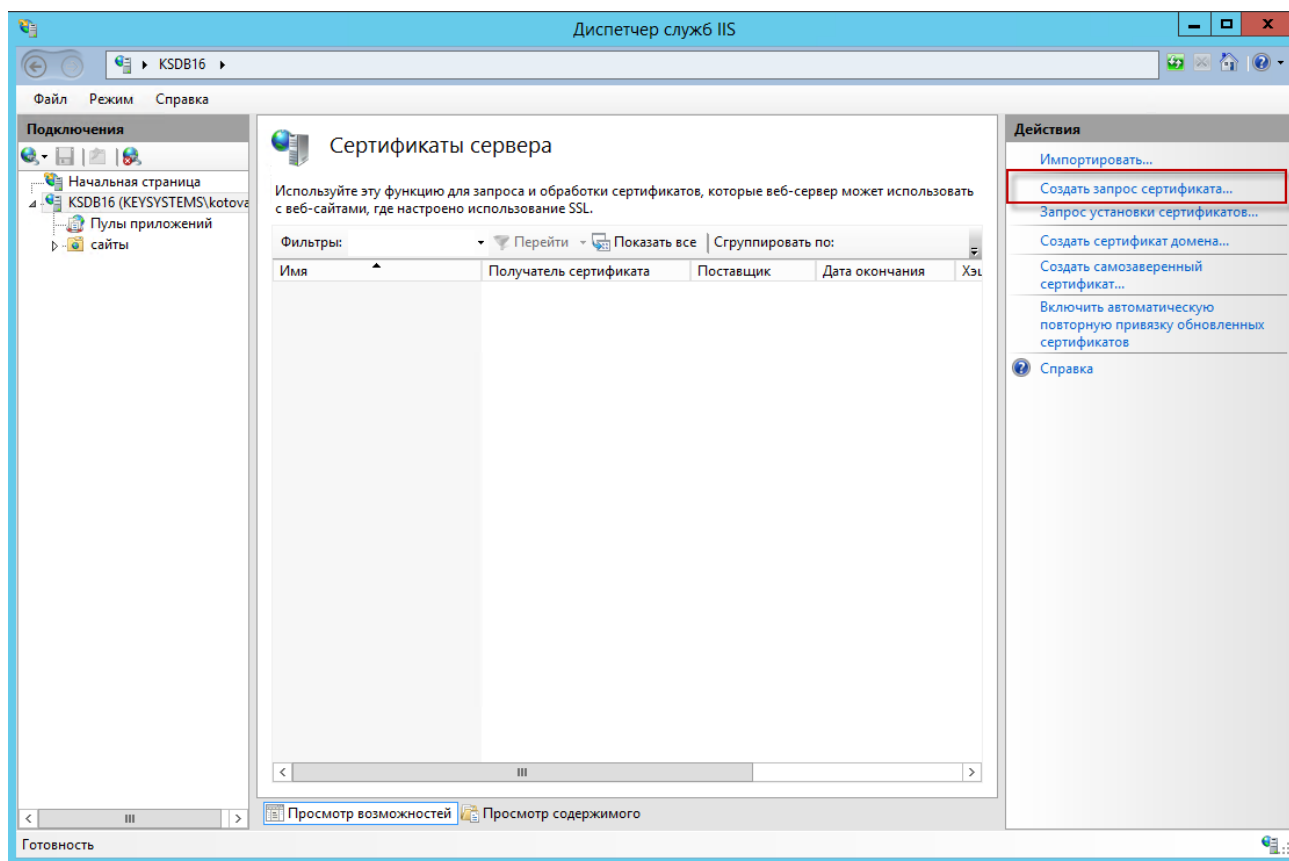
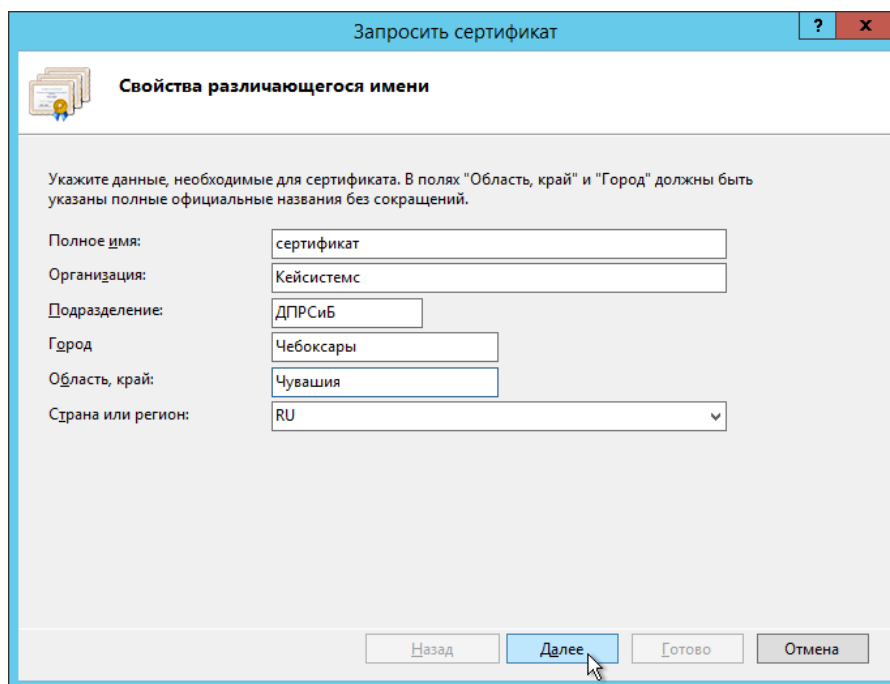


Рисунок 4. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (Рисунок 5):

- **Полное имя** - адрес ресурса;
- **Организация**;
- **Подразделение** – не является обязательным для заполнения;
- **Город**;
- **Область**;
- **Страна или регион** - обозначение страны (на латинице);



Запросить сертификат

Свойства различающегося имени

Укажите данные, необходимые для сертификата. В полях "Область, край" и "Город" должны быть указаны полные официальные названия без сокращений.

Полное имя:

Организация:

Подразделение:

Город:

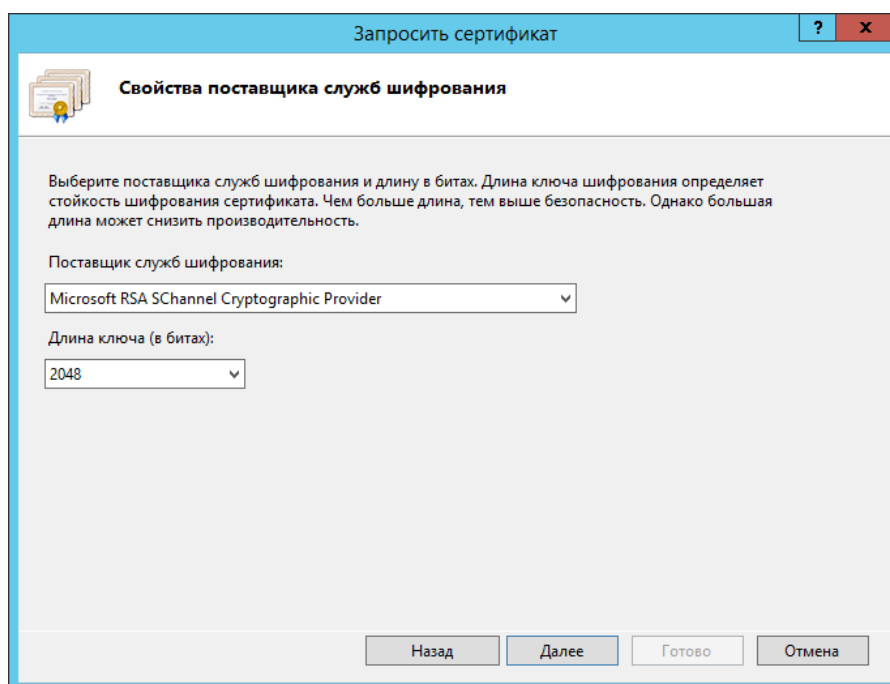
Область, край:

Страна или регион:

Назад Далее Готово Отмена

Рисунок 5. Свойства имени сертификата

Далее выберите значение длины ключа - 2048 бит (Рисунок 6).



Запросить сертификат

Свойства поставщика служб шифрования

Выберите поставщика служб шифрования и длину в битах. Длина ключа шифрования определяет стойкость шифрования сертификата. Чем больше длина, тем выше безопасность. Однако большая длина может снизить производительность.

Поставщик служб шифрования:

Длина ключа (в битах):

Назад Далее Готово Отмена

Рисунок 6. Свойства поставщика служб шифрования

Укажите место сохранения CSR запроса (это будет обычный текстовый файл *.txt) (Рисунок 7).

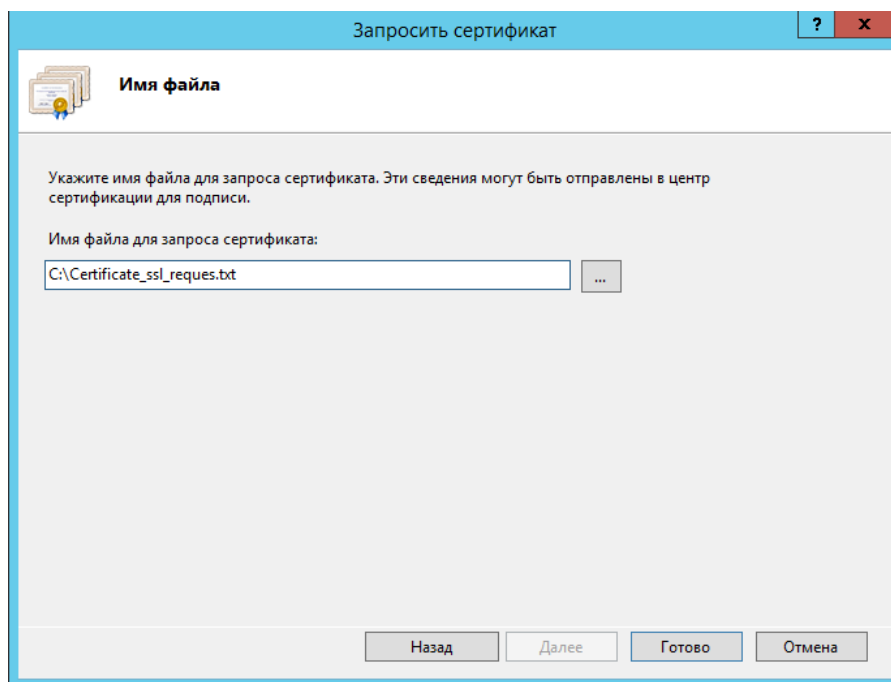


Рисунок 7. Путь к месту сохранения CSR запроса

Полученный от центра сертификации сертификат, будет необходимо настроить под IIS, так как ему потребуется формат rfx.

1.2.2. Создание самозаверенного сертификата

В открывшемся окне, в области «Действия», выберите опцию «Создать самозаверенный сертификат» (Рисунок 8).

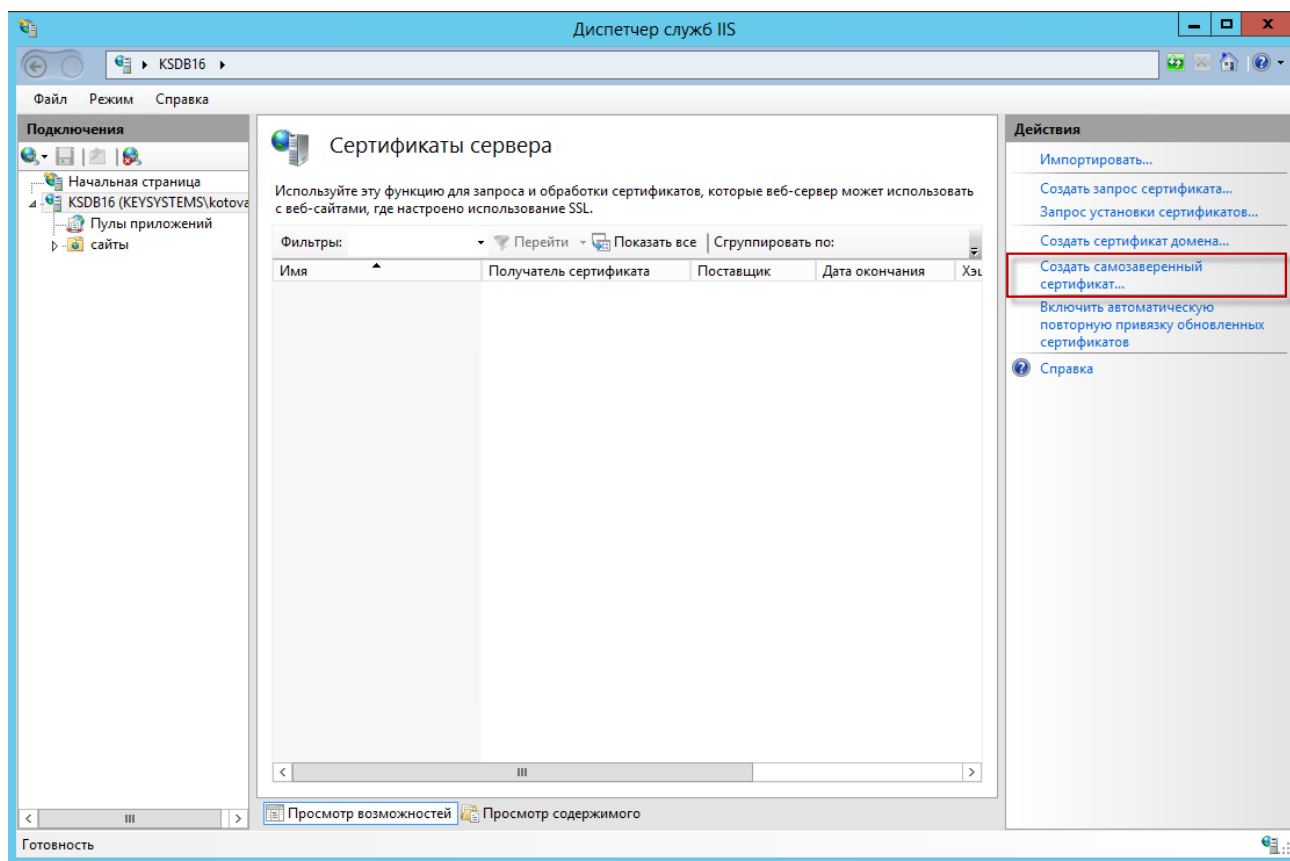


Рисунок 8. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (Рисунок 9):

- **Понятное имя** – идентификатор сертификата;
- **Выбрать хранилище сертификатов** - укажите значение «Личный», оно подойдет для стандартного размещения (значение «Размещение веб-служб» используется для SNI технологии).

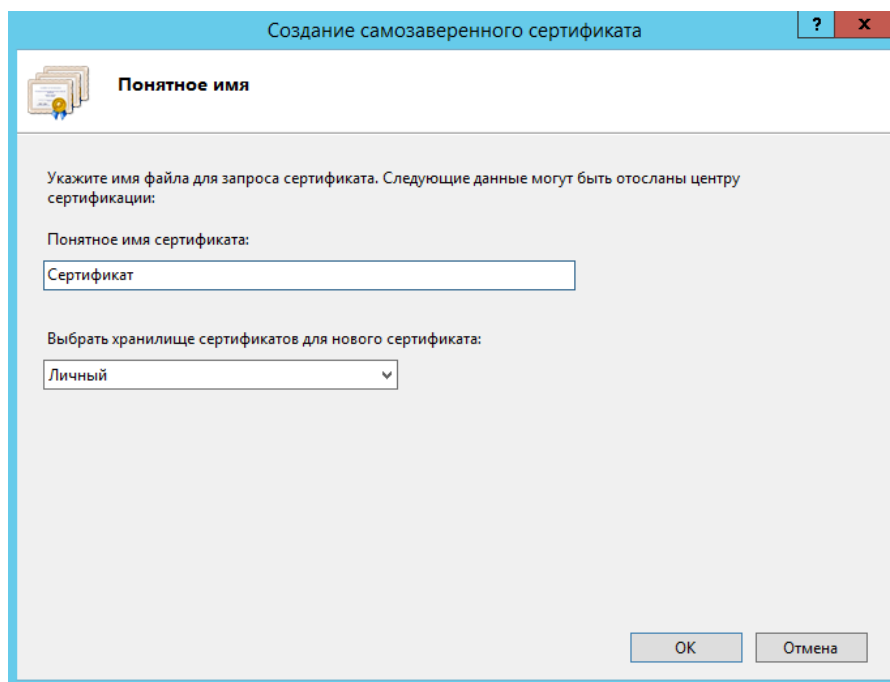


Рисунок 9. Свойства имени сертификата

По кнопке [ОК] сертификат сразу отобразится в списке «Сертификаты сервера» (Рисунок 10).

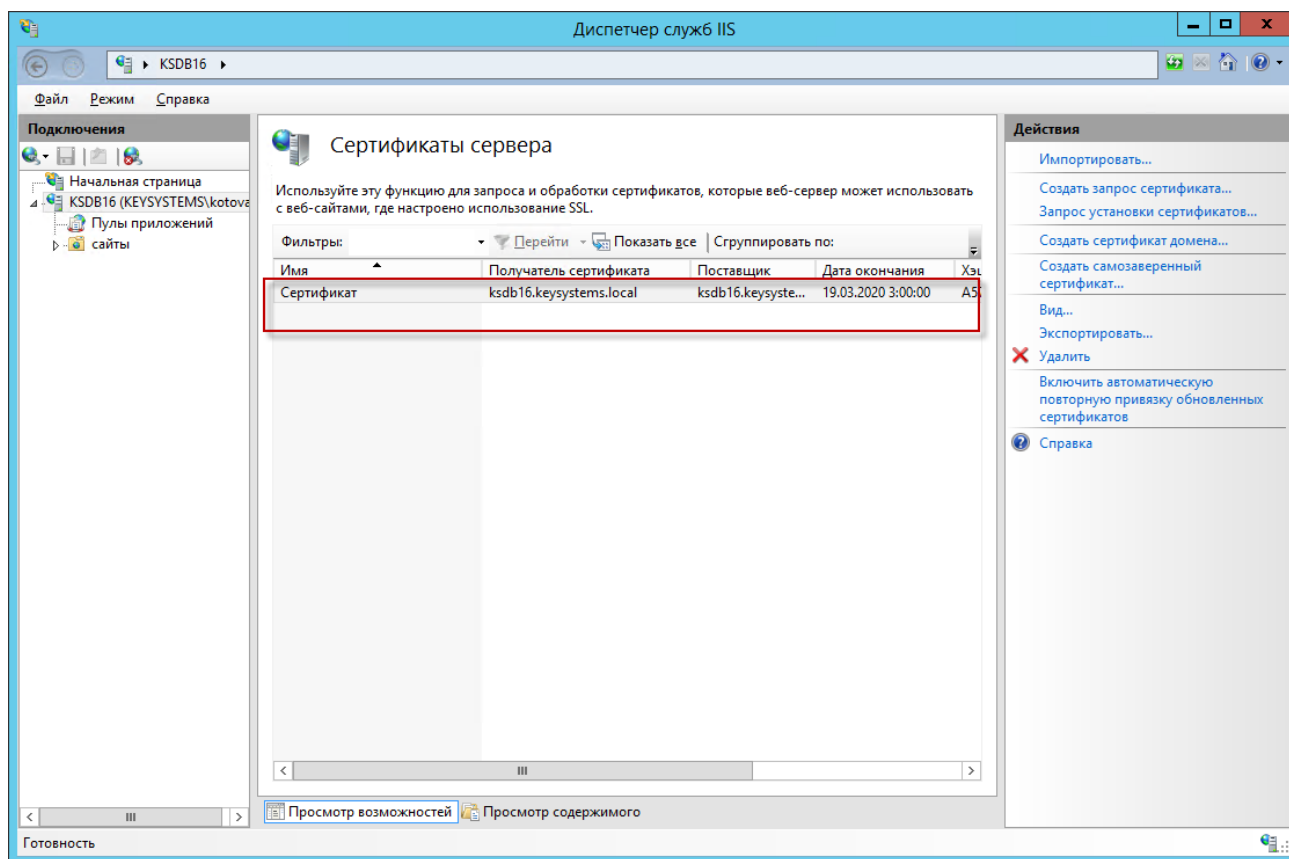


Рисунок 10. Сертификаты сервера

1.3. Установка SSL в PFX

Для дальнейшей работы необходимо импортировать нужный сертификат. Откройте диспетчер IIS и перейдите в окно «Сертификаты сервера» (см. Рисунок 10). В открывшемся окне, в области «Действия», выберите опцию «Импортировать». В режиме «Обзор» выберите pfx архив (Рисунок 11).

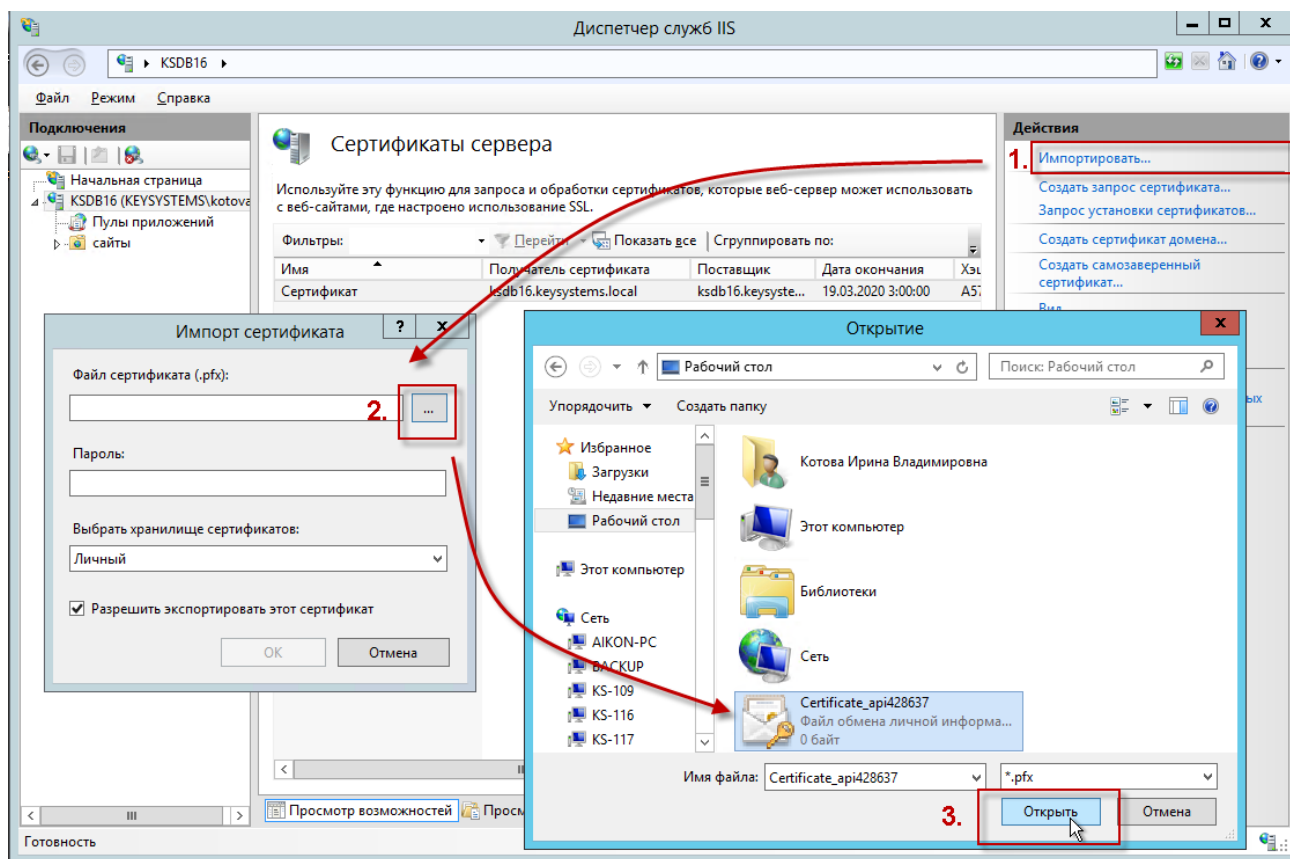


Рисунок 11. Подготовка к импорту сертификата

Пароль - укажите пароль;

Выбрать хранилище сертификатов - укажите значение «Личный», оно подойдет для стандартного размещения (значение «Размещение веб-служб» используется для SNI технологии).

Импорт будет выполнен по кнопке [ОК] (Рисунок 12).

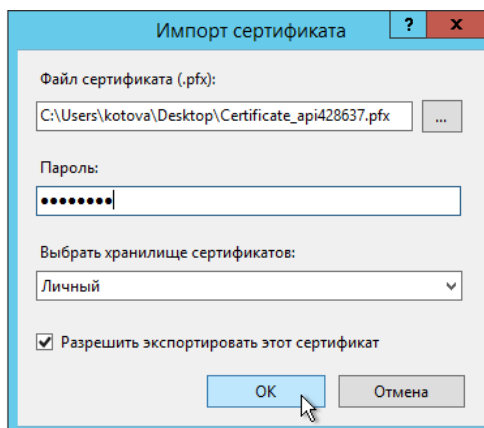


Рисунок 12. Импорт сертификата

Далее выберите каталог «сайты» и по щелчку правой кнопкой мыши по соответствующей строке выберите в контекстном меню пункт «Изменить привязки» для настройки протокола https в IIS (Рисунок 13).

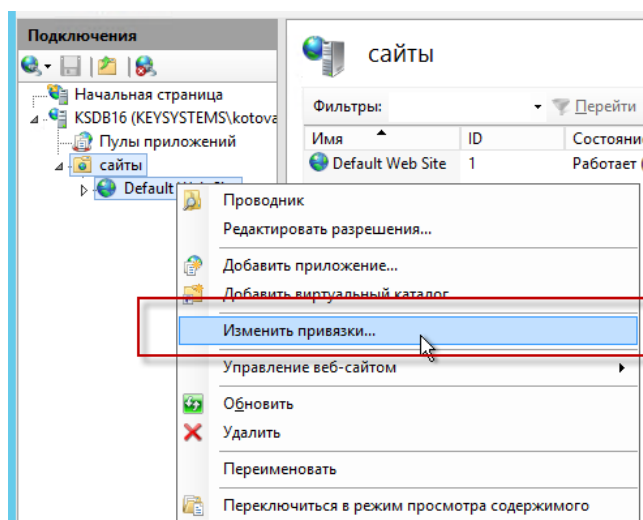


Рисунок 13. Настройка протокола https в IIS

Укажите для сайта (Рисунок 14):

- **Тип** - https и номер порта, по умолчанию, это порт 443 (убедитесь, что он открыт в брандмауэре);
- **Имя узла** - укажите полное название сайта;
- **SSL-сертификат** - выберите импортированный сертификат и сохраните настройки.

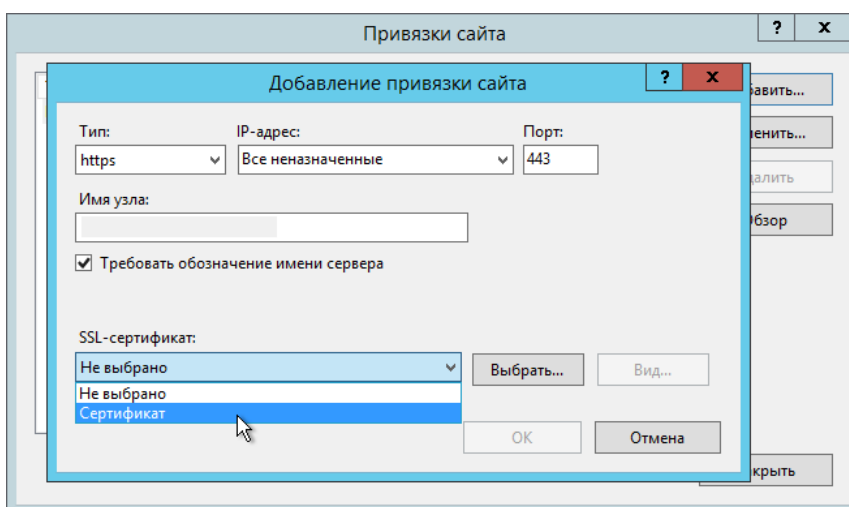


Рисунок 14. Добавление привязки сайта

В завершение проверьте сайт по протоколу HTTPS: в адресной строке должен отобразиться закрытый замок. Это означает, что ssl сертификат установлен в IIS правильно (Рисунок 14).

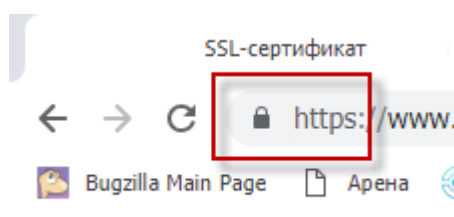


Рисунок 15. Проверка корректности установки сертификата

ГЛОССАРИЙ

Certificate Signing Reques (CSR) запрос - запрос на получение сертификата, который представляет собой текстовый файл, содержащий в закодированном виде информацию об администраторе домена и открытый ключ.

Secure Sockets Layer (SSL) - сертификат – уровень защищенных сокетов – уникальная цифровая подпись сайта. Такой сертификат нужен любым организациям, работающим с персональными данными для предотвращения несанкционированного доступа к информации.

HTTPS (HyperText Transfer Protocol Secure) – это расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол SSL или TLS. По умолчанию HTTPS использует 443 TCP-порт (для незащищенного HTTP используется порт 80).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Термин
1	2
ПК	Программный комплекс
CSR	Certificate Signing Request, запрос на получение сертификата
SSL	Secure Sockets Layer, уровень защищенных сокетов
PFX	Формат, предназначенный для хранения ключевой пары, который распознается и используется браузерами и почтовыми агентами

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	20.03.2019	Белоносов А.А.