

Описание процедуры подключения и настройки файлового шлюза к СОД Оператора криптоплатформы IMEX

Подключение файлового шлюза к СОД Оператора криптоплатформы IMEX

1. Файловый шлюз Системы Обмена Документами Оператора криптоплатформы IMEX (далее – СОД) представляет собой приложение, предназначенное для обмена файлами. Клиентское приложение, файловый шлюз (FG.Client2) устанавливается на стороне Участника торгов, через который происходит обмен файлами с сервером IMEX. Приложение отправляет и получает файлы, подключившись к одному из файловых шлюзов. Файловый шлюз и рабочие каталоги программы задаются в настройках приложения FG.Client2.

- Если в папке выходных файлов есть файлы, приложение отправляет их на сервер IMEX. Для отправки документа требуется поместить его в папку выходных файлов (по умолчанию /out) и начать обработку в приложении;
- Если файлы получены Участником торгов от сервера IMEX, приложение загружает их в папку входных файлов (по умолчанию /in). Для того, чтобы получить файлы, необходимо запустить обработку в приложении.

Файловый шлюз может работать в двух режимах: как приложение и как служба. Документооборот на стороне Участника торгов разделен на 6 различных шлюзов на 1 сервере СОД. После добавления сертификата в систему СОД вам будет отправлен список адресов СОД, которые используются для настройки файлового шлюза и обмена сообщениями, где FIRMM — пятибуквенный идентификатор участника СОД.

2. Для установки файлового шлюза необходимо скачать последнюю версию дистрибутива программы с сайта IMEX <https://imexchange.tech/...../FileGate2.0.7.zip> и распаковать архив в рабочую папку.

Программное обеспечение файлового шлюза работает в Windows с установленной платформой .NET Framework 4.0.

3. Запустите **FG.Client2.exe** и настройте его в соответствии с приведенными ниже инструкциями по настройке файлового шлюза. Для этого необходимо указать сертификат пользователя, присвоенный ему адрес СОД, сохранить настройки программы и установить сертификат сервера IMEX (см. пункт 3 **Инструкции по настройке файлового шлюза**). Для каждого адреса СОД должен быть настроен отдельный экземпляр файлового шлюза.

Для того, чтобы отправлять сообщения на другие адреса, необходимо создать папку для каждого получателя с именем, состоящим из адреса клиента в папке выходных файлов (по умолчанию **.\out**). Все файлы в этом каталоге будут отправлены на тот же адрес, что и имя папки. Например, для того, чтобы отправлять сообщения в адрес **IMEX@REGISTER**, должна быть создана директория **.\out\IMEX@REGISTER**.

Для одного файлового шлюза параметры аналогичны для всех организаций, с которыми осуществляется обмен документами.

Дистрибутив файлового шлюза уже включает в себя стандартные каталоги (out\...) для отправки файлов:

Адрес	Описание
Для обмена документами с Оператором криптоплатформы IMEX	
IMEX@REGISTER	Регистрация заявлений, отчетов, уведомлений и иных документов. Регистрация клиентов, заявление CLIENTS
IMEX@REPORT	Предоставление отчетов, уведомлений, выписок

IMEX@LOGIN	Заявление на регистрацию логина, ТКС для логина
IMEX@BOOKING	Заявления на бронирование Краткого кода клиента
IMEX@ONLINE	Заявления на активацию ранее забронированного Краткого кода клиента
IMEX@CLIENT	Обмен неформализованной документации
IMEX@KYC	Направление в IMEX идентификационных данных по клиенту

4. Проверьте работоспособность файлового шлюза, отправив тестовый файл на свой адрес СОД с помощью кнопки «**Ручная обработка**» (см. пункт 4 **Инструкции по настройке файлового шлюза**).

5. Запись об успешной работе должна отображаться в окне программы и в текстовом файле журнала. Если файл был успешно отправлен, вы можете запросить новые сообщения с сервера с помощью этой же кнопки. Если произошла ошибка и вы не можете исправить ее самостоятельно, обратитесь в службу технической поддержки:

Электронная почта: support@imexchange.tech

6. Для работы веб-интерфейса <https://edo.imexchange.tech/Edo/> требуется установленная на компьютере библиотека Caricom версии 2.1.0.2, доступная для скачивания по ссылке:

<https://imexchange.tech/...../CAPICOM-KB931906-v2102.zip>

Вход в веб-интерфейс осуществляется с помощью сертификата пользователя СОД.

В настоящее время он позволяет отслеживать историю обмена сообщениями СОД, загружать ESIG, проверять подписывающую сторону и даты истечения срока действия ESIG.

Структура каталогов FileGate

Шлюз на стороне Участника FIRMM	FIRMM шлюзы		под папка для обмена с Оператором криптоплатформы IMEX
	REGISTER	in	IMEX@REGISTER
		out	IMEX@REGISTER
	REPORT	in	IMEX@REPORT
			IMEX@CLIENT
		out	IMEX@REPORT
			IMEX@CLIENT
	LOGIN	in	IMEX@LOGIN
		out	IMEX@LOGIN
	BOOKING	in	IMEX@BOOKING
		out	IMEX@BOOKING
	ONLINE	in	IMEX@ONLINE
		out	IMEX@ONLINE
	KYC	in	IMEX@KYC
		out	IMEX@KYC

Инструкции по настройке файлового шлюза

1. Настройка файловых шлюзов в FG. Программа Client2:

- Актуальную версию программного обеспечения можно скачать на сайте IMEX:

<https://imexchange.tech/.../FileGate2.0.7.zip>

Программное обеспечение не требует установки. Необходимо распаковать архив, содержащий приложение, в выбранную директорию и запустить файл FG. Client2.exe.

- Отдельный экземпляр FG.Client2 должен использоваться для **каждого** файлового шлюза (FIRMM@REGISTER, FIRMM@REPORT, FIRMM@LOGIN, FIRMM@BOOKING, FIRMM@ONLINE, FIRMM@KYC), каждый из которых работает из своего каталога.
- Если один и тот же файловый шлюз будет использоваться разными операторами, рекомендуется создать общий сетевой каталог для получения файлов и локальные каталоги для каждого пользователя для отправки. *(В противном случае полученные файлы будут помещены в локальное хранилище файловым шлюзом, на котором обработка будет начата в первую очередь).*
- Принцип работы и запуск файлового шлюза: файловый шлюз может быть запущен в двух режимах: Однократный запуск — кнопка **Ручная обработка** на вкладке *Главная* запускает разовую обработку.

Автоматический запуск — кнопка **Начать автоматическую обработку** на вкладке *Главная* запускает периодическую обработку, в которой можно настроить период пула каталогов по полю Период опроса каталогов (в секундах).

Принцип работы: когда начинается обработка, файловый шлюз опрашивает каталоги на предмет исходящих сообщений на стороне участника на наличие файлов, и если файлы есть, отправляет их в папку для получения на стороне получателя. Затем, если есть файлы, доступные для получения участником, он загружает их в каталог входящих файлов, указанный участником.

- Программа должна быть запущена с правами системного администратора. Для начала работы следует правильно задать требуемые параметры с помощью элементов управления, параметры для всех файловых шлюзов разные.

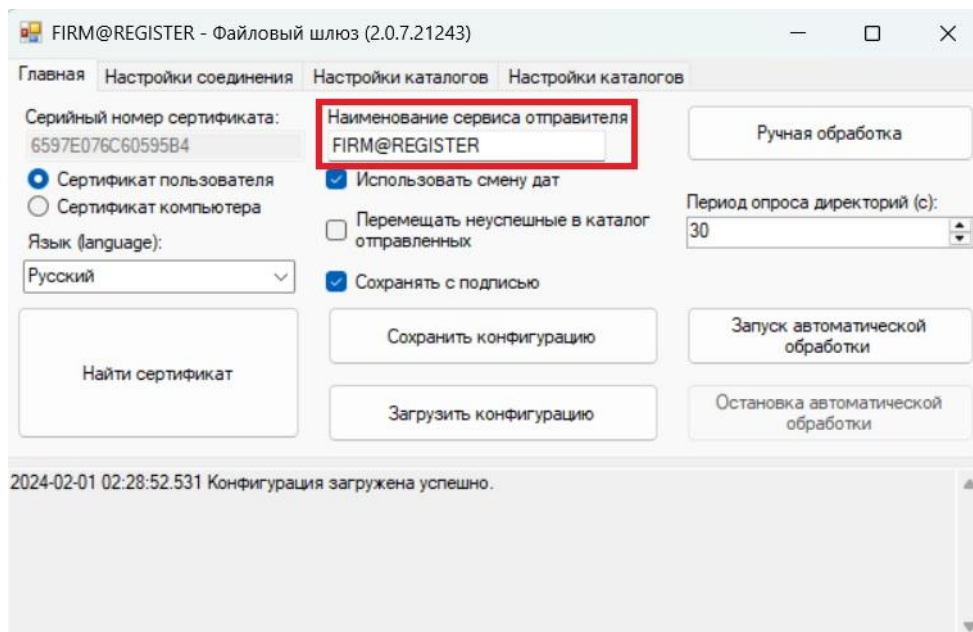
Настройка файловых шлюзов:

- [FIRMM@REGISTER](#)
- [FIRMM@REPORT](#)
- [FIRMM@LOGIN](#)
- [FIRMM@BOOKING](#)
- [FIRMM@ONLINE](#)
- [FIRMM@KYC](#)

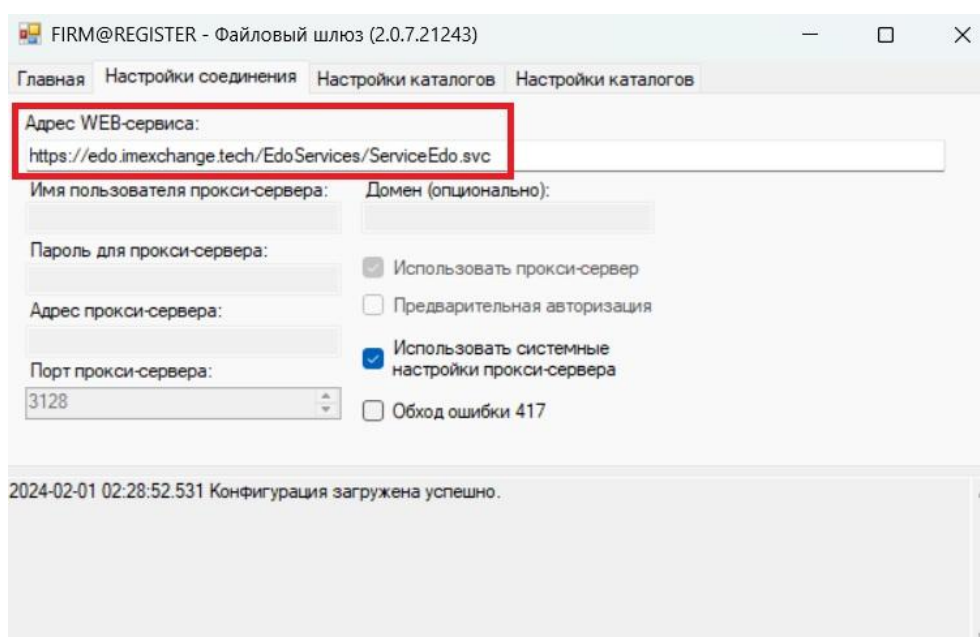
После изменения каких-либо настроек необходимо **сохранить конфигурацию** на вкладке **«Главная»!**

A) FIRMM@REGISTER

В поле Имя клиентской службы на вкладке Главная необходимо ввести FIRMM@REGISTER, где FIRMM — пятибуквенный идентификатор участника.



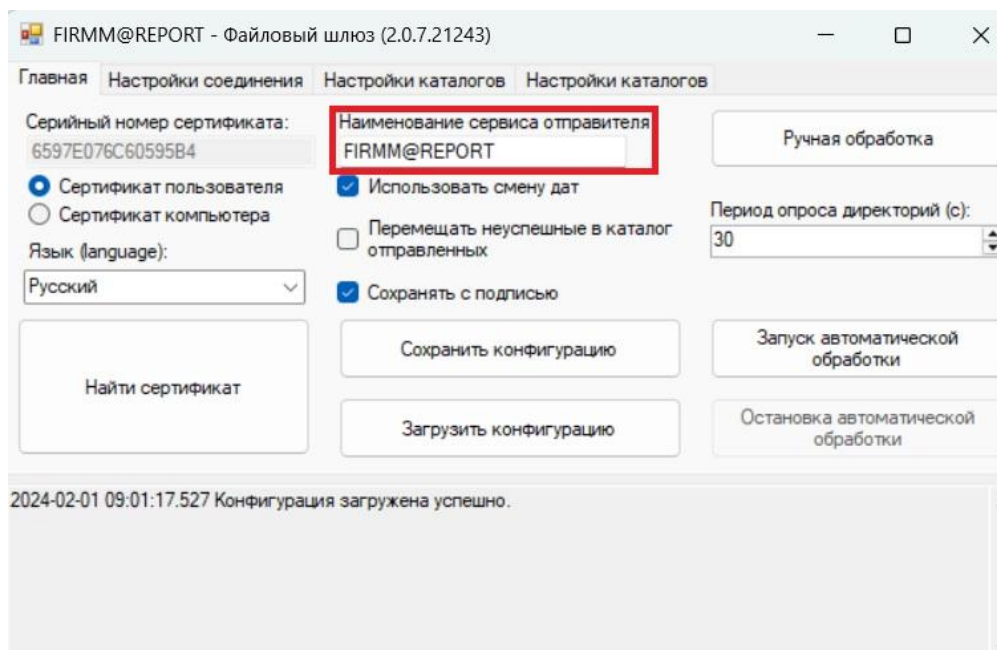
В поле WEB-адрес на вкладке Настройки подключения необходимо ввести следующий адрес: <https://edo.imexchange.tech/EdoServices/ServiceEdo.svc> (для подключения к шлюзу тестовой площадки СОД необходимо ввести адрес: <https://edo-test.imexchange.tech/EdoServices/ServiceEdo.svc>).



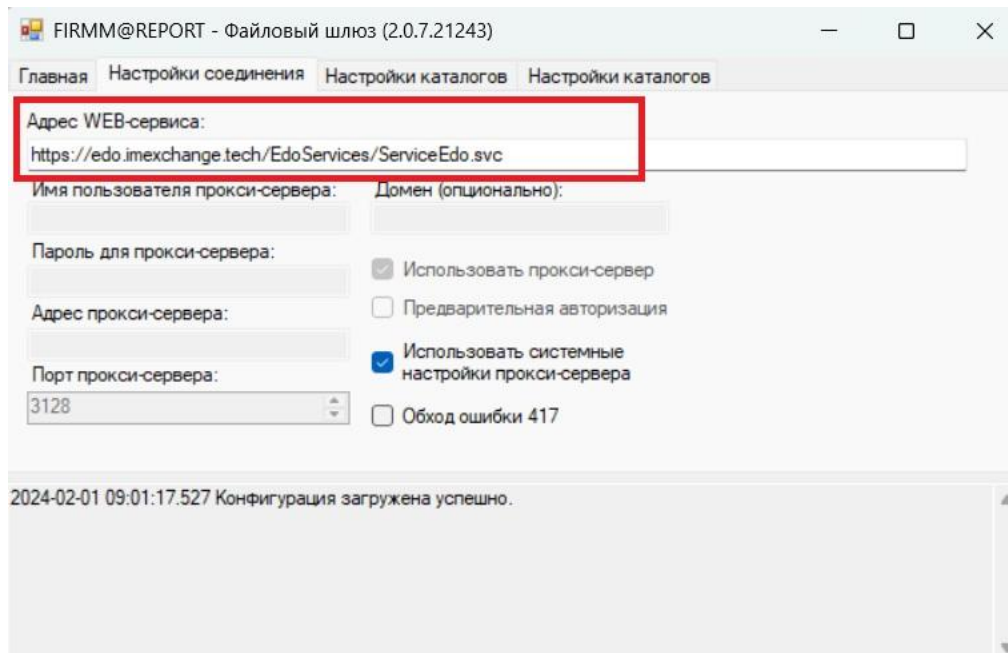
На вкладке *Настройки папок* необходимо указать отдельные каталоги входящих и исходящих сообщений для этого файлового шлюза. Папка выходных файлов должна содержать папку с именем: IMEX@REGISTER. Именно в эту папки следует направлять файлы для отправки на соответствующий файловый шлюз. Каталоги для входящих и исходящих сообщений могут иметь произвольные имена, папки для конкретных файловых шлюзов будут создаваться автоматически после обработки файлов для отправки/получения. Сертификат сервера может быть общим для всех файловых шлюзов. Кроме того, убедитесь, что учетная запись Windows, на которой выполняется FG.Client2 имеет права доступа ко всем указанным каталогам.

Б) FIRMM@REPORT

В поле *Имя клиентской службы* на вкладке *Главная* необходимо ввести FIRMM@REPORT, где FIRMM — пятибуквенный идентификатор участника.



В поле *WEB-адрес* на вкладке *Настройки подключения* необходимо ввести следующий адрес: <https://edo.imexchange.tech/EdoServices/ServiceEdo.svc> (для подключения к шлюзу тестовой площадки СОД необходимо ввести адрес: <https://edo-test.imexchange.tech/EdoServices/ServiceEdo.svc>).

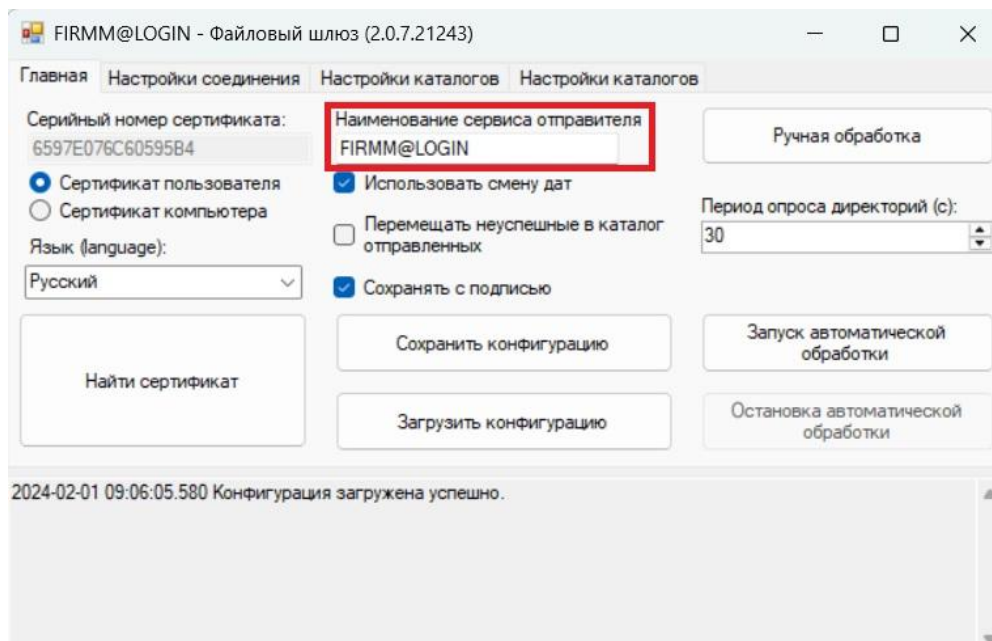


На вкладке *Настройки папок* необходимо указать отдельные каталоги входящих и исходящих сообщений для этого файлового шлюза. Папка выходных файлов должна содержать две папки с именами: IMEX@REPORT и IMEX@CLIENT. Именно в эти папки следует направлять файлы для отправки на соответствующие файловые шлюзы. Каталоги для входящих и исходящих сообщений могут иметь произвольные имена, папки для конкретных файловых шлюзов будут создаваться автоматически после обработки файлов для отправки/получения. Сертификат сервера может быть общим для всех файловых

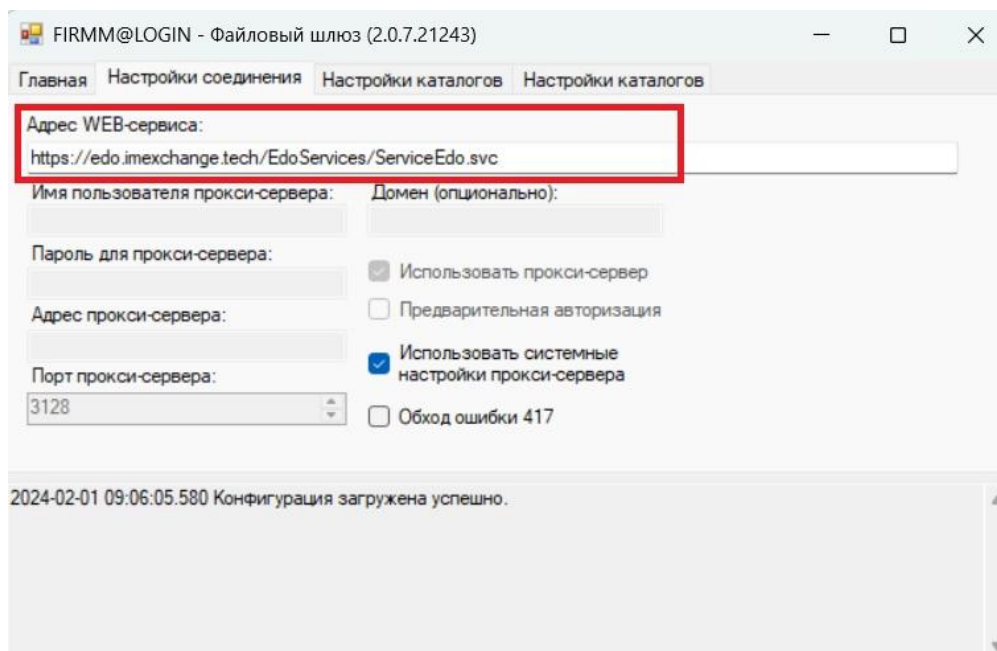
шлюзов. Кроме того, убедитесь, что учетная запись Windows, на которой выполняется FG.Client2 имеет права доступа ко всем указанным каталогам.

В) FIRMM@LOGIN

В поле *Имя клиентской службы* на вкладке *Главная* необходимо ввести FIRMM@LOGIN, где FIRMM — пятибуквенный идентификатор участника.



В поле *WEB-адрес* на вкладке *Настройки подключения* необходимо ввести следующий адрес: <https://edo.imexchange.tech/EdoServices/ServiceEdo.svc> (для подключения к шлюзу тестовой площадки СОД необходимо ввести адрес: <https://edo-test.imexchange.tech/EdoServices/ServiceEdo.svc>).

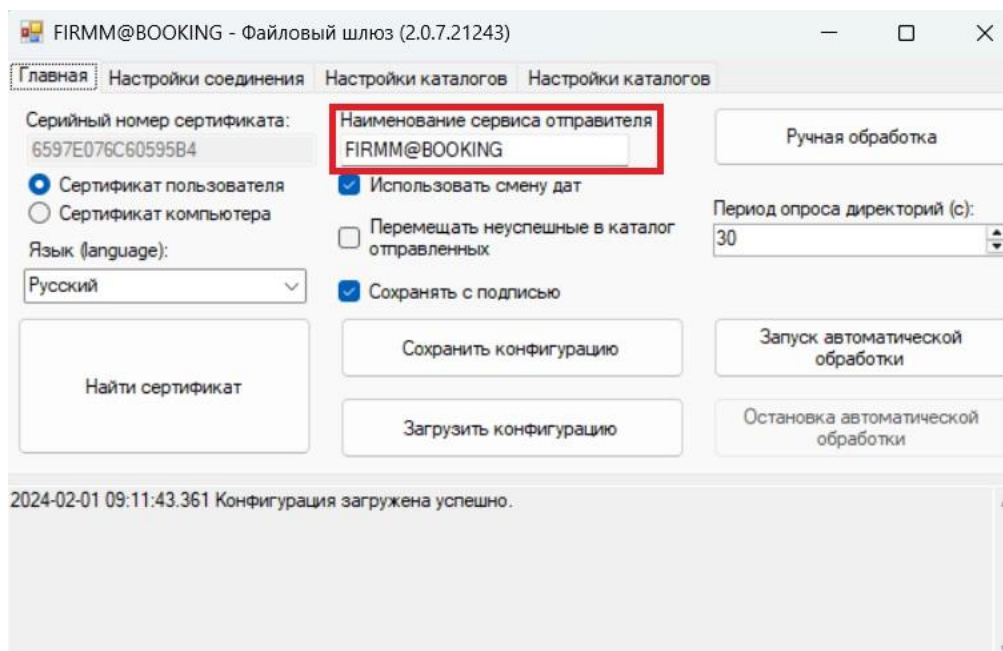


На вкладке *Настройки папок* необходимо указать отдельные каталоги входящих и исходящих сообщений для этого файлового шлюза. Папка выходных файлов должна содержать папку с именем: IMEX@LOGIN. Именно в эту папки следует направлять файлы для отправки на соответствующий файловый шлюз. Каталоги для входящих и исходящих сообщений могут иметь произвольные имена, папки для конкретных файловых шлюзов будут создаваться автоматически после обработки файлов для

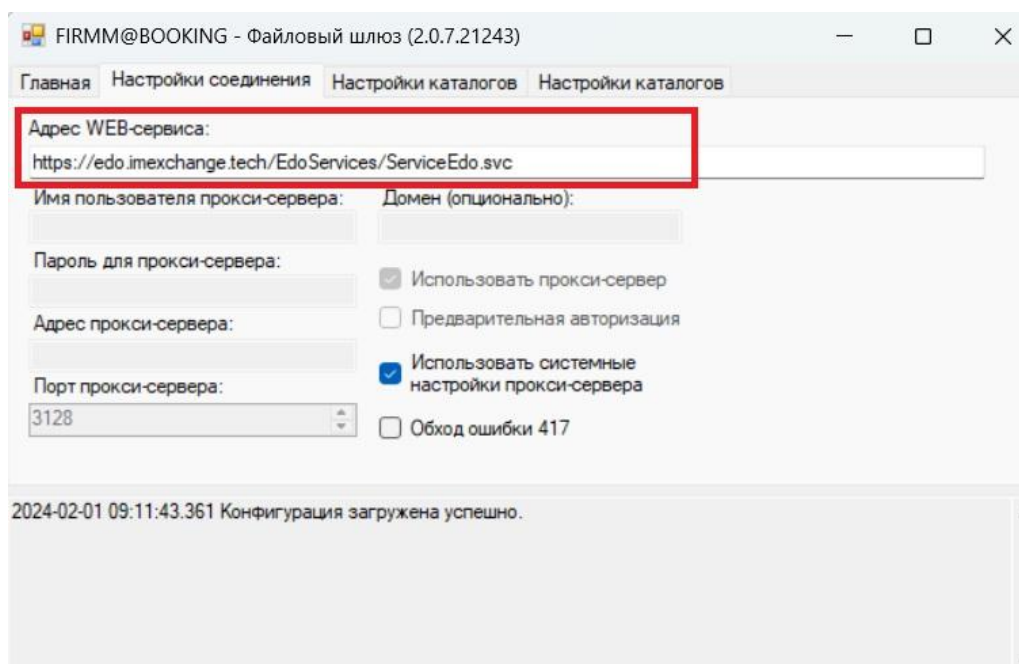
отправки/получения. Сертификат сервера может быть общим для всех файловых шлюзов. Кроме того, убедитесь, что учетная запись Windows, на которой выполняется FG.Client2 имеет права доступа ко всем указанным каталогам.

Г) FIRMM@BOOKING

В поле *Имя клиентской службы* на вкладке *Главная* необходимо ввести FIRMM@BOOKING, где FIRMM — пятибуквенный идентификатор участника.



В поле *WEB-адрес* на вкладке *Настройки подключения* необходимо ввести следующий адрес: <https://edo.imexchange.tech/EdoServices/ServiceEdo.svc> (для подключения к шлюзу тестовой площадки СОД необходимо ввести адрес: <https://edo-test.imexchange.tech/EdoServices/ServiceEdo.svc>).

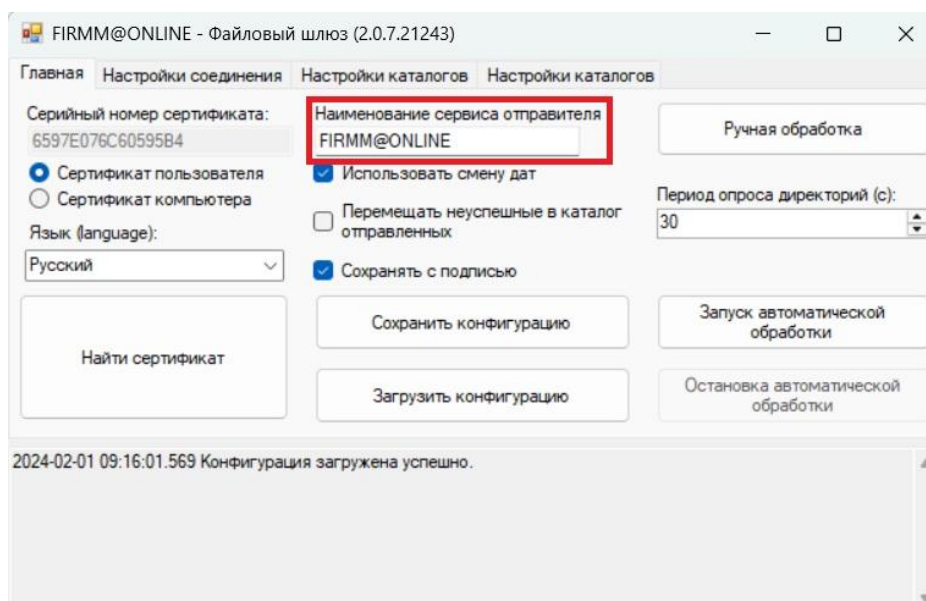


На вкладке *Настройки папок* необходимо указать отдельные каталоги входящих и исходящих сообщений для этого файлового шлюза. Папка выходных файлов должна содержать папку с именем: IMEX@BOOKING. Именно в эту папки следует направлять файлы для отправки на соответствующий файловый

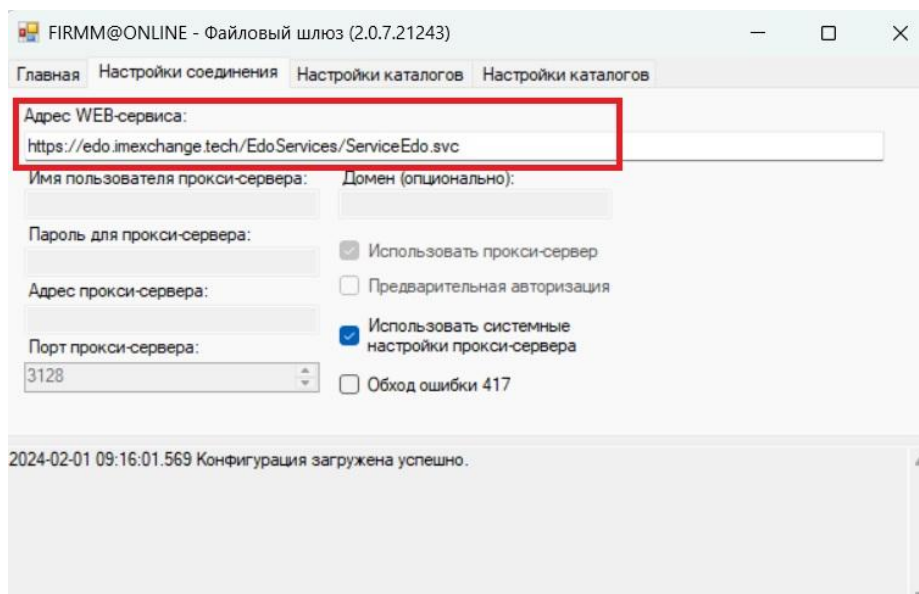
шлюз. Каталоги для входящих и исходящих сообщений могут иметь произвольные имена, папки для конкретных файловых шлюзов будут создаваться автоматически после обработки файлов для отправки/получения. Сертификат сервера может быть общим для всех файловых шлюзов. Кроме того, убедитесь, что учетная запись Windows, на которой выполняется FG.Client2 имеет права доступа ко всем указанным каталогам.

Д) FIRMM@ONLINE

В поле *Имя клиентской службы* на вкладке *Главная* необходимо ввести FIRMM@ONLINE, где FIRMM — пятибуквенный идентификатор участника.



В поле WEB-адрес на вкладке *Настройки подключения* необходимо ввести следующий адрес: <https://edo.imexchange.tech/EdoServices/ServiceEdo.svc> (для подключения к шлюзу тестовой площадки СОД необходимо ввести адрес: <https://edo-test.imexchange.tech/EdoServices/ServiceEdo.svc>).

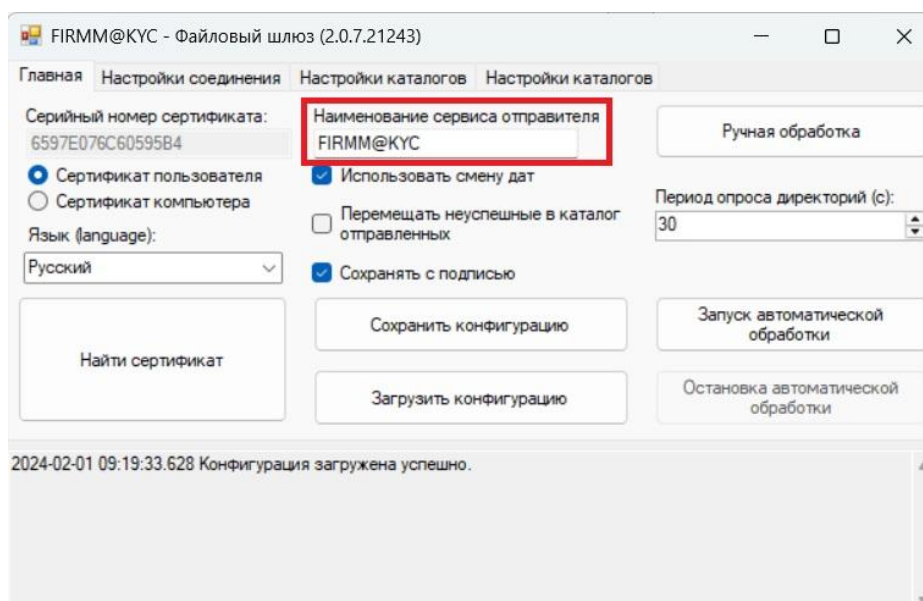


На вкладке *Настройки папок* необходимо указать отдельные каталоги входящих и исходящих сообщений для этого файлового шлюза. Папка выходных файлов должна содержать папку с именем: IMEX@ONLINE. Именно в эту папки следует направлять файлы для отправки на соответствующий файловый

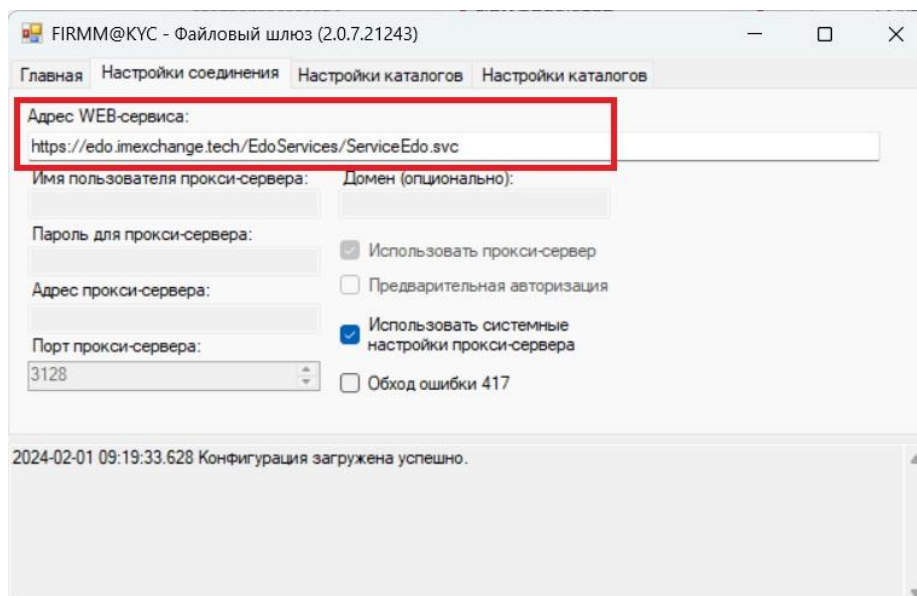
шлюз. Каталоги для входящих и исходящих сообщений могут иметь произвольные имена, папки для конкретных файловых шлюзов будут создаваться автоматически после обработки файлов для отправки/получения. Сертификат сервера может быть общим для всех файловых шлюзов. Кроме того, убедитесь, что учетная запись Windows, на которой выполняется FG.Client2 имеет права доступа ко всем указанным каталогам.

Е) FIRMM@KYC

В поле *Имя клиентской службы* на вкладке *Главная* необходимо ввести FIRMM@KYC, где FIRMM — пятибуквенный идентификатор участника.



В поле WEB-адрес на вкладке *Настройки подключения* необходимо ввести следующий адрес: <https://edo.imexchange.tech/EdoServices/ServiceEdo.svc> (для подключения к шлюзу тестовой площадки СОД необходимо ввести адрес: <https://edo-test.imexchange.tech/EdoServices/ServiceEdo.svc>).



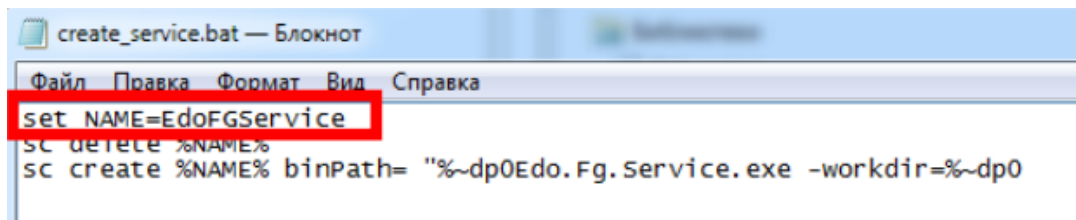
На вкладке *Настройки папок* необходимо указать отдельные каталоги входящих и исходящих сообщений для этого файлового шлюза. Папка выходных файлов должна содержать папку с именем: IMEX@KYC. Именно в эту папки следует направлять файлы для отправки на соответствующий файловый

шлюз. Каталоги для входящих и исходящих сообщений могут иметь произвольные имена, папки для конкретных файловых шлюзов будут создаваться автоматически после обработки файлов для отправки/получения. Сертификат сервера может быть общим для всех файловых шлюзов. Кроме того, убедитесь, что учетная запись Windows, на которой выполняется FG.Client2 имеет права доступа ко всем указанным каталогам.

После изменения каких-либо настроек необходимо сохранить конфигурацию на вкладке «Главная»

2. Запуск файлового шлюза как службы:

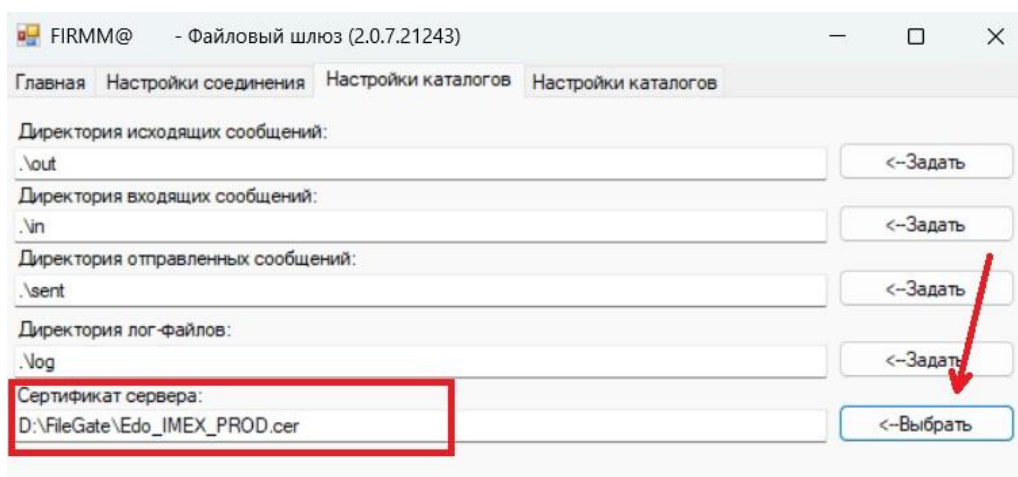
Запуск приложения в качестве службы Windows выполняется, если требуется, чтобы файловый шлюз запускался автоматически при запуске Windows и работал в фоновом режиме. *Имя папки, в которой запускается приложение, не должно содержать пробелов.* В каталоге, содержащем файловый шлюз, есть файл с именем create_service.bat, который можно использовать для запуска приложения в качестве службы Windows. Чтобы отредактировать его, щелкните правой кнопкой мыши по файлу и выберите в контекстном меню пункт «Редактировать». Если необходимо запустить несколько приложений, каждое из них должно иметь собственное имя службы (задайте параметр NAME).



3. Настройка сертификатов:

Для того, чтобы использовать файловый шлюз, необходимо использовать сертификат сервера IMEX и собственный сертификат.

Вам необходимо скачать **сертификат сервера IMEX** по следующей ссылке, так как он может быть обновлен: https://imexchange.tech/.../EDO_IMEX_PROD.zip. Вам нужно поместить сертификат сервера в любую директорию и указать путь к этому файлу в FG.Client2 на вкладке *Настройки папок*, также нужно убедиться, что FG.Client2 имеет доступ к каталогу с сертификатом сервера.

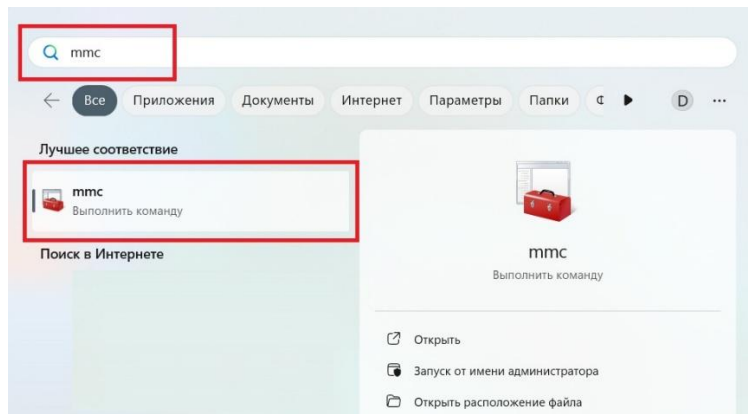


В случае, если вам необходимо заменить или добавить свой собственный сертификат открытого RSA-ключа, вам необходимо добавить его на стороне Оператора криптоплатформы IMEX. Ваш **собственный сертификат_открытого RSA-ключа** (файл с расширением *.crt в zip-архиве) и при наличии сертификаты всей цепочки доверенных центров верификации, которые находятся в вашем собственном

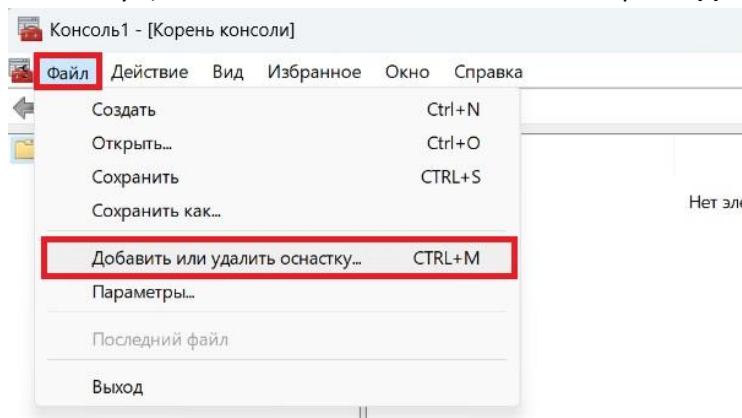
сертификате, должны быть отправлены support@imexchange.tech. Сертификаты следует отправлять в архиве .zip, так как почтовые серверы и клиенты могут блокировать отправку сертификатов.

Ваш собственный сертификат закрытого RSA-ключа (файл с расширением *.pfx) также должен быть добавлен в Персональные сертификаты и Доверенные корневые центры сертификации.

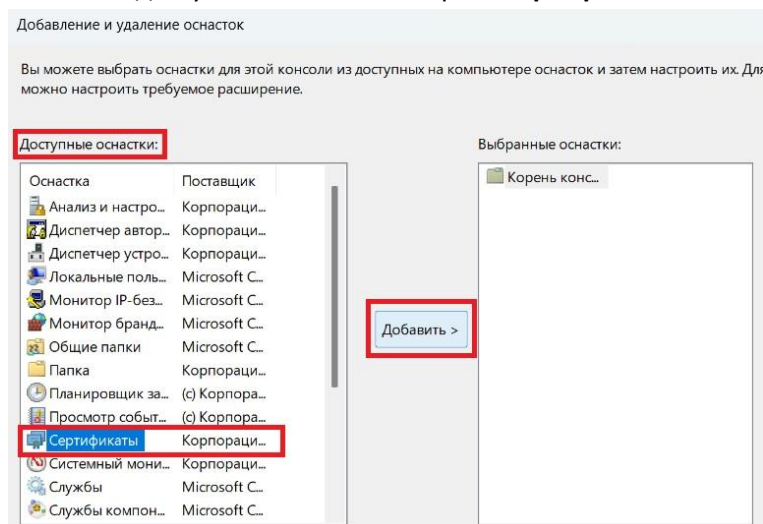
- на панели задач в окне поиска ввести «mmc» и далее выбрать предложенное меню «mmc»



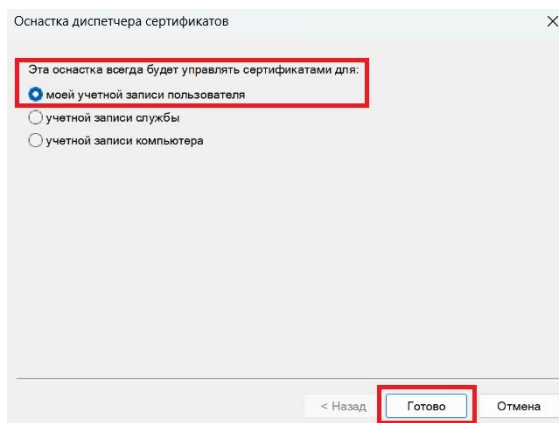
- в запущенной консоли нажать «Файл» и выбрать «Добавить или удалить оснастку...»



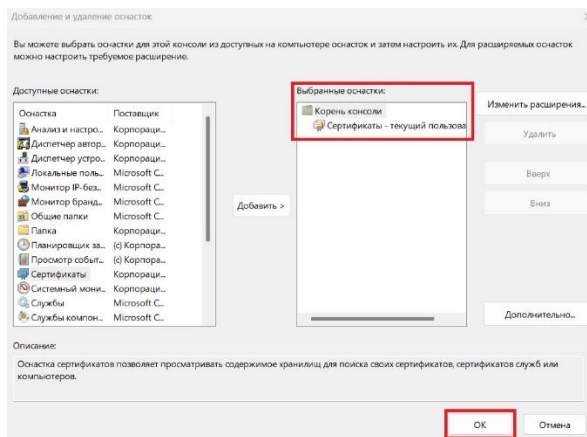
- в списке доступных оснасток выбрать Сертификаты и нажать «Добавить»



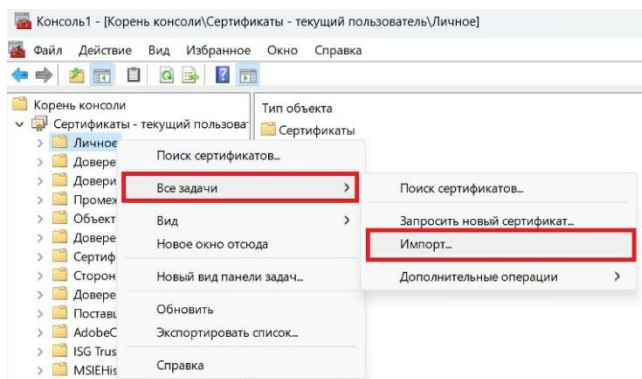
- выбрать управление сертификатами для: моей учетной записи пользователя и нажать «Готово»



- далее нажать «ОК»



- правой кнопкой мыши вызвать контекстное меню и выбрать «Все задачи» -> «Импорт...»



- запуститься Мастер импорта сертификата, нажать «Далее»

Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

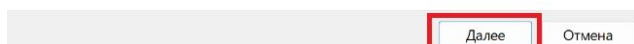
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

☒ Текущий пользователь

☐ Локальный компьютер

Для продолжения нажмите кнопку "Далее".



- выбрать импортируемый файл **сертификат закрытого RSA-ключа** (файл с расширением *.pfx)

Импортируемый файл

Укажите файл, который вы хотите импортировать.

Имя файла:

D:\Key_for_IMEX.pfx

Обзор...

Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:

Файл обмена личной информацией - PKCS #12 (.PFX, .P12)

Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)

Хранилище сериализованных сертификатов (.SST)

Далее

Отмена

- ввести пароль закрытого ключа, который был введен на этапе Экспорта (Инструкция_по_генерации_RSA_ключа_и_сертификата_для_ЭДО.pdf) и нажать «Далее». Для защиты не стоит отмечать ключ как экспортируемый (второй пункт – Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его)

Защита с помощью закрытого ключа

Для обеспечения безопасности закрытый ключ защищен паролем.

Введите пароль для закрытого ключа.

Пароль:

☐ Показывать пароль

Параметры импорта:

☐ Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.

☐ Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.

☐ Защита закрытого ключа с помощью безопасной виртуализации (неэкспортируемый)

☒ Включить все расширенные свойства.

Далее

Отмена

- выбрать хранилище сертификатов – Личное и нажать «Далее»

Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

☐ Автоматически выбрать хранилище на основе типа сертификата

☒ Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Личное

Обзор...

Далее

Отмена

- на экране Завершения мастера импорта сертификатов проверить Тип хранилища – Личное, Содержимое – PFX, и Путь к файлу. Завершить импорт нажатием «Готово»

Завершение мастера импорта сертификатов

Сертификат будет импортирован после нажатия кнопки "Готово".

Были указаны следующие параметры:

Хранилище сертификатов, выбранное пользователем	Личное
Содержимое	PFX
Файл	D:\Key_for_IMEX.pfx

Готово Отмена

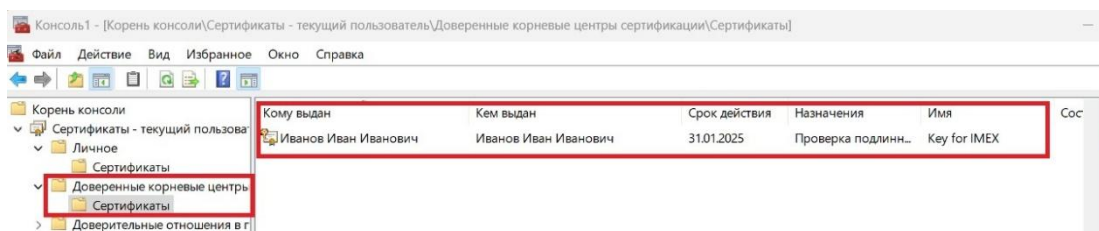
Мастер импорта сертификатов



Импорт успешно выполнен.

OK

- в оснастке **Сертификаты** можно визуально проверить добавленный сертификат, проверьте что значок сертификата имеет следующий вид



Повторите описанные выше шаги для добавления Вашего собственного сертификата закрытого RSA-ключа (файл с расширением *.pfx) в **Доверенные корневые центры сертификации**, для этого на этапе выбора хранилища измените тип на **Доверенные корневые центры сертификации** как указано на картинке ниже

Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

☐ Автоматически выбрать хранилище на основе типа сертификата

☒ Поместить все сертификаты в следующее хранилище

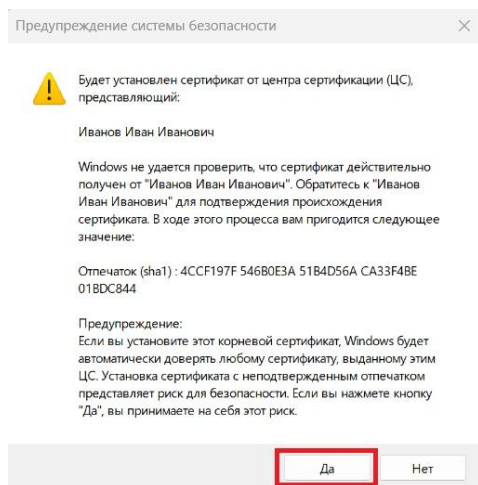
Хранилище сертификатов:


Доверенные корневые центры сертификации

Обзор...

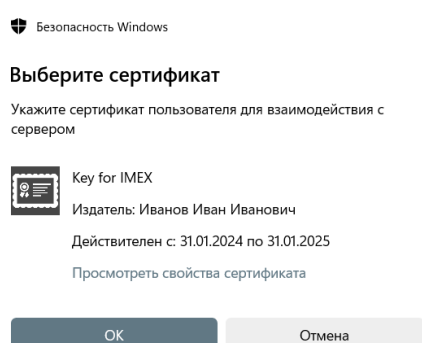
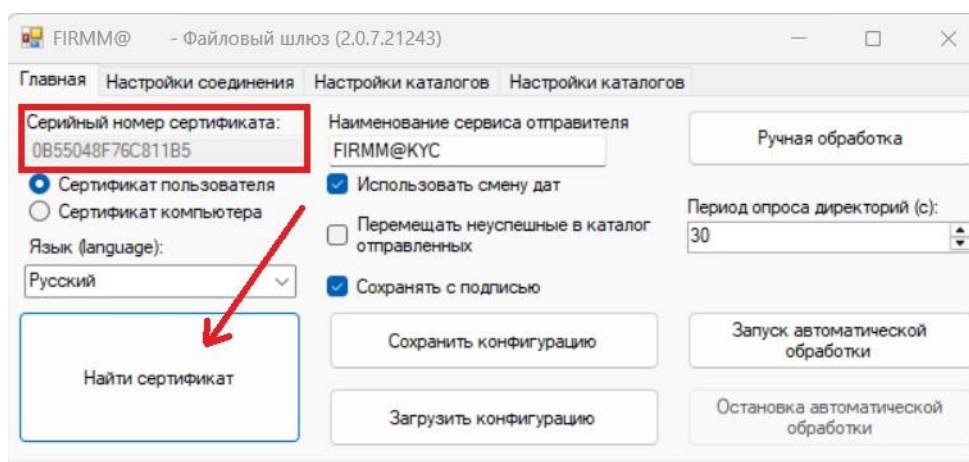
Далее Отмена

- на экране предупреждение системы безопасности нажмите «Да»



- в оснастке **Сертификаты** можно визуальнo проверить добавленный сертификат, проверьте что значок сертификата имеет следующий вид 

После добавления собственного сертификата закрытого RSA-ключа необходимо на вкладке *Главная* нажать кнопку *Найти сертификат* и выбрать действительный сертификат, который был зарегистрирован на серверах СОД. Один сертификат можно использовать для работы с несколькими файловыми шлюзами СОД.



4. Тестирование файлового шлюза электронного документооборота:

Вы можете отправить файл самому себе для тестирования шлюза. Для этого необходимо:

- А) В директории исходящих сообщений создайте папку с именем, соответствующим *полю* Имя клиентской службы на вкладке *Главная*.
- Б) Поместите любой файл (не более 40Мб) в созданную папку.

- В) Затем следует дважды запустить ручную обработку на вкладке *Главная*, либо запустить автоматическую обработку и подождать 2 "периода опроса каталогов" (*при первом запуске файл обрабатывается для отправки, во втором - для получения*).
- Г) Если все настроено правильно, файл появится в каталоге входящих сообщений в папке с именем, соответствующим полю Имя клиентской службы.

5. Типичные ошибки и способы их решения:

- А) **Текст ошибки:** Несоответствие сертификата между сервером и ответным сертификатом.

Причина: Сертификат сервера не был обновлен.

Решение: Необходимо скачать актуальную версию сертификата

https://imexchange.tech/.../EDO_IMEX_PROD.zip, затем на вкладке Настройки папок в поле Сертификат сервера указать путь к этому файлу, затем Сохранить конфигурацию на вкладке Главная.

- Б) **Текст ошибки:** Служба не найдена или отключена.

Причины: 1. Адрес WEB-сервиса указан неверно.

2. Участник не зарегистрирован в данном файловом шлюзе.

Решения: 1. Укажите корректный адрес WEB-сервиса (*Второй пункт в FIRMM@GATE Параметры шлюза*)

2. Электронная почта support@imexchange.tech обратиться за консультацией по получению доступа к файловому шлюзу.

- В) **Текст ошибки:** Не удалось инициализировать веб-сервис: Ошибка авторизации.

Причина: Публичная часть сертификата участника на стороне сервера IMEX не указана.

Решение: Отправьте сертификат в zip-архиве на support@imexchange.tech с просьбой установить этот сертификат в СОД.

- Г) **Текст ошибки:** Сбой инициализации криптосистемы: сертификат не найден или недействителен для подписи.

Причина: Во время проверки цепочки сертификатов были обнаружены ошибки.

Решение: Необходимо проверить корректность установки сертификатов в хранилище Персонального и Доверенного корневых центров сертификации, целостность цепочки сертификатов, переустановить сертификаты для создания корректной цепочки. Также необходимо убедиться в том, что закрытый ключ установлен и ЭЦП с этим ключом подключена к ПК.

Если сертификат установлен в реестре, убедитесь в наличии закрытого ключа.

- Д) **Текст ошибки:** ошибка проверки каталога.

Причина: Сетевая папка, на которую ссылаются каталоги, указанные на вкладке *Настройки папок*, или если на этой вкладке есть незаполненные поля, отключена.

Решение: Повторно подключитесь к сетевой папке или заполните путь в полях на вкладке *Настройки папок*.

- Е) **Текст ошибки:** Ошибка вызова WEB-сервиса:

Причина: В сети возникли проблемы с конфигурацией прокси-сервера.

Решение: Выполните корректную настройку прокси-сервера и проверьте наличие WEB-адресов СОД серверов.