Инструкция по настройке рабочего места клиента

для работы в системе «NS-FiXit» АО Банк «Национальный стандарт»

I. Первичная настройка системы

1. Для работы системы необходимо установить на компьютер Java версии 1.8.220 и выше.
2. **Для работы в системе используется браузер Internet Explorer**

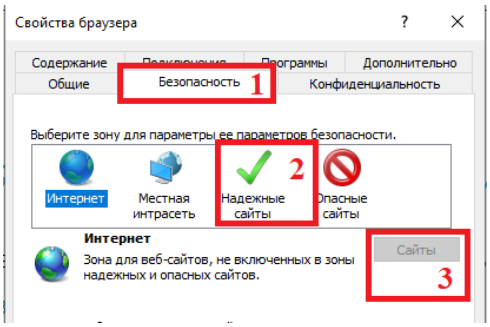
Примечание:

В современных операционных системах семейства Windows ярлык Internet Explorer надо добавить на рабочий стол в ручном режиме. Для этого надо:

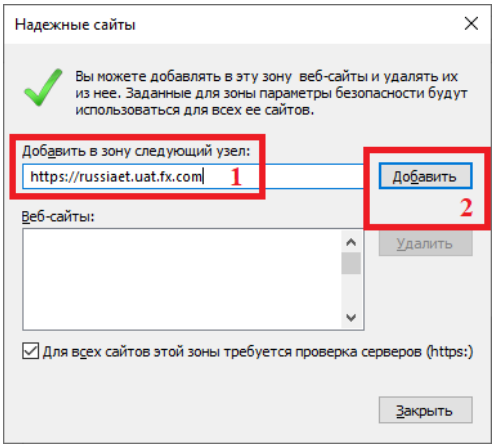
- *Зайти в каталог «C:\Program Files (x86)\Internet Explorer» и щелкнуть правой кнопкой мышки по файлу iexplore.exe.*
- *В открывшемся меню выбрать пункт: Отправить\ Рабочий стол (создать ярлык)*

3. Зайти по ссылке https://ns-bank.fx.com/client.html
4. Выполнить настройки Internet Explorer. Для этого надо нажать значок  и в открывшемся меню выбрать пункт «Свойства браузера».

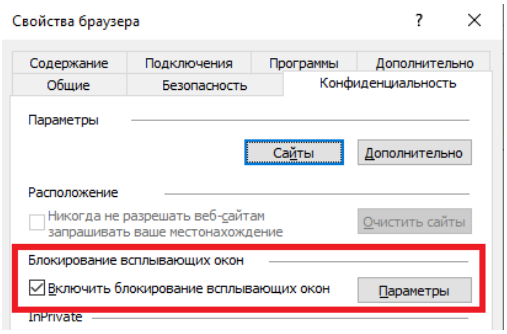
4.1. В открывшемся окне перейти на закладку безопасность. Выбрать пиктограмму «Надежные сайты». Чуть ниже и правее станет доступна кнопка «Сайты».



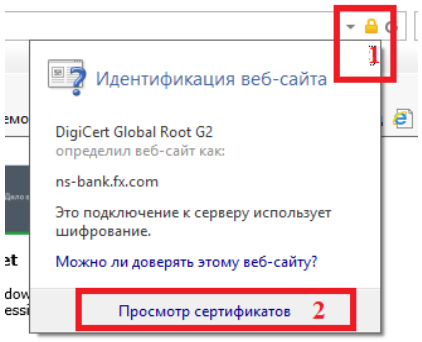
4.2. В окне настроек «Надежных сайтов» ввести адрес сайта услуги https://ns-bank.fx.com/client.html в поле «Добавить в зону следующий узел» и нажать кнопку «Добавить»



4.3. Проверить на закладке «Конфиденциальность» включение функционала блокирования всплывающих окон. Если включено (установлен флаг), добавить сайт в исключения по аналогии с п.4.2 .



5. Открыть сертификат сайта для просмотра. Для этого в правой части адресной строки щелкнуть левой кнопкой мыши по пиктограмме 🔒 и в открывшемся окне выбрать пункт «Просмотр сертификатов».



6. В открывшемся окне сертификата нажать кнопку «Установить сертификат». В мастере установки все параметры определяются автоматически и настроек не требуют.
7. Перейти на закладку «Состав» и нажать кнопку «Копировать в файл». Сохранить сертификат в файл.
8. Настроить Java

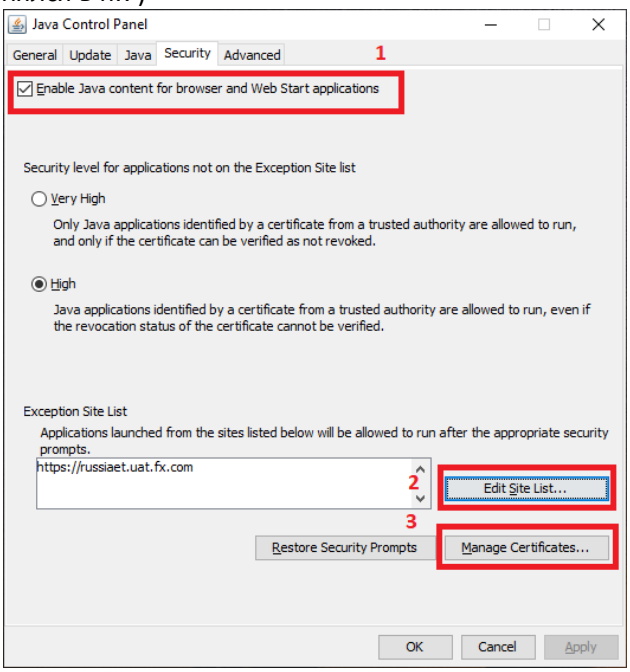
8.1. Открыть Java Control Panel через меню «Пуск \ Java \ Configure Java».

8.2. Перейти на закладку security.

8.3. Если отсутствует, то установить флаг «Enable Java content for brouser and Web Start applications» (на рисунке ниже обозначено 1)

8.4. Добавить сайт в список разрешенных. Нажать кнопку «Edit Site List…», ввести адрес сайта услуги https://ns-bank.fx.com/client.html в поле «Location» и нажать кнопку «OK»

8.5. Добавить сертификат в доверенные. Нажать кнопку «Manage Certificates…», импортировать сертификат из файла (сохранялся в п.7)



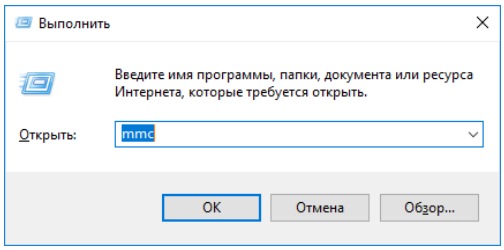
9. Перезапустить Internet Explorer и войти в систему.
10. При первом запуске потребуется ожидание примерно 2-3 минуты, пока откроется окно программы.

II. Инструкция по созданию запроса и импорту электронного сертификата

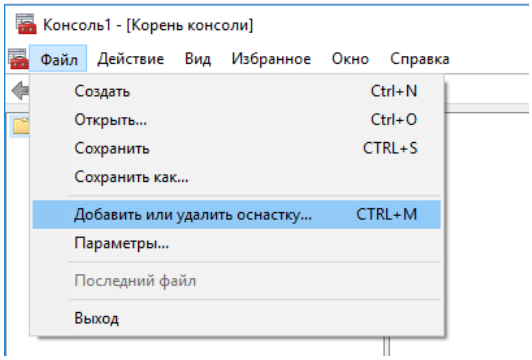
1. Создание запроса на сертификат

Для получения сертификата необходимо сформировать файл запроса на сертификат и направить его в Банк. Для этого необходимо выполнить следующие действия:

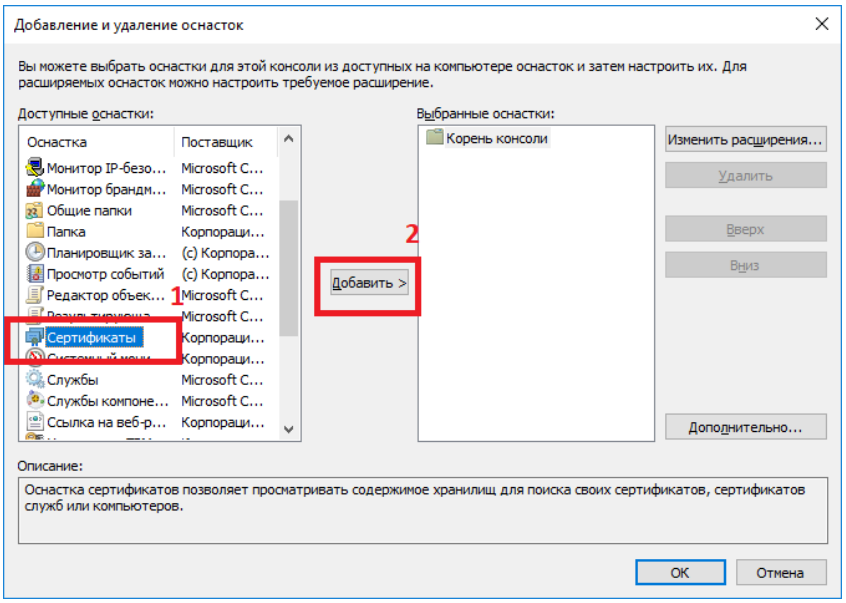
1.1. Запустить консоль управления Windows. Для этого щелкнуть правой кнопкой мышки по кнопке «Пуск», выбрать пункт меню «Выполнить», в открывшемся окне набрать команду «mmc» и нажать кнопку «ОК»:



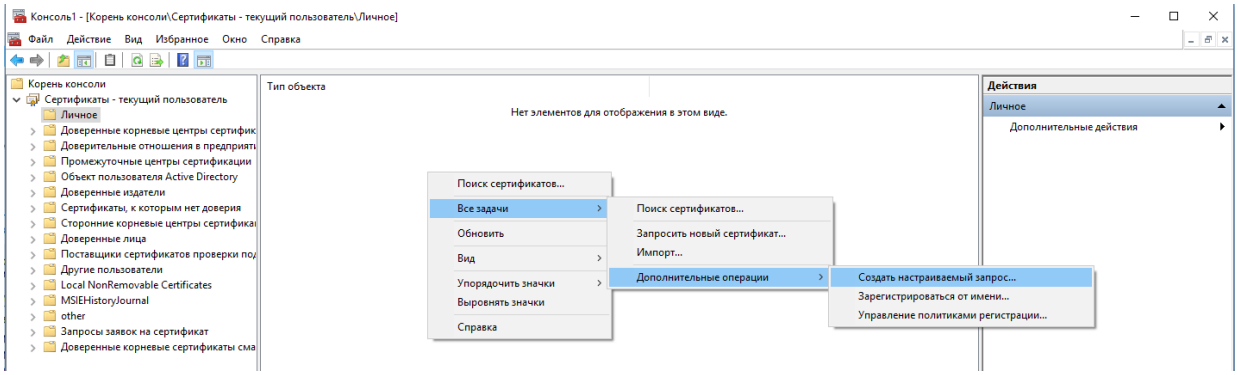
1.2. В открывшемся окне надо выбрать пункт меню «Файл → Добавить или удалить оснастку»:



1.3. На экране откроется окно выбора оснастки. В левой части окна надо выбрать пункт «Сертификаты» и нажать кнопку «Добавить»:

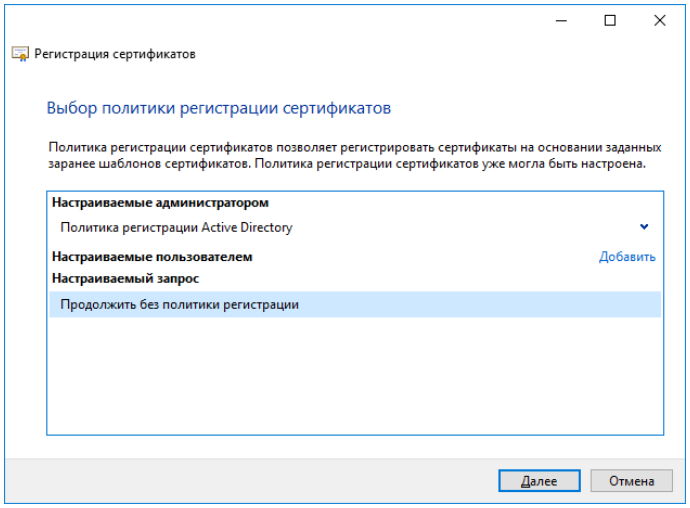


1.4. В левой части консоли выбрать раздел «Личное» и в средней части консоли кликнуть правой кнопкой мышки по свободному месту. В открывшемся меню выбрать пункт меню «Все задачи → Дополнительные операции → Создать настраиваемый запрос»:



1.5. В открывшемся окне нажать кнопку «Далее».

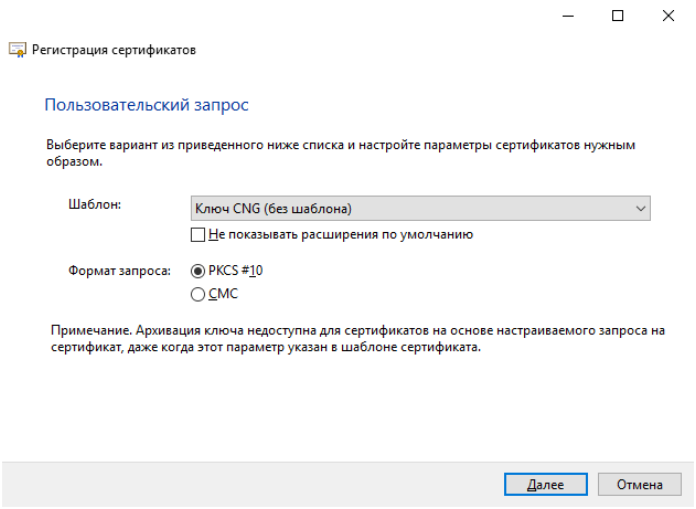
1.6. Выбрать пункт «Продолжить без политики регистрации» и нажать кнопку «Далее»:



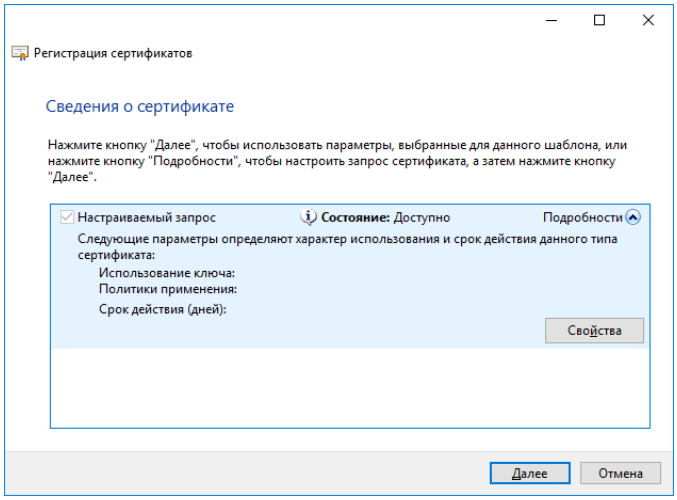
1.7. На следующем экране убедиться в том, что настройки установлены следующим образом:

- Шаблон: «Ключ CNG (без шаблона)»
- Формат запроса: «PKCS #10»

И нажать кнопку «Далее»:

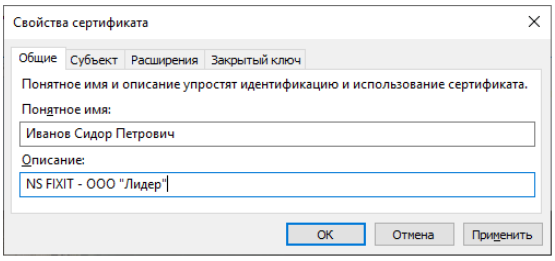


1.8. В окне «Сведения о сертификате» открыть расширенную информацию о запросе, нажав кнопку «Подробности» и нажать кнопку «Свойства»:



1.9. На закладке «Общее» заполнить поля:

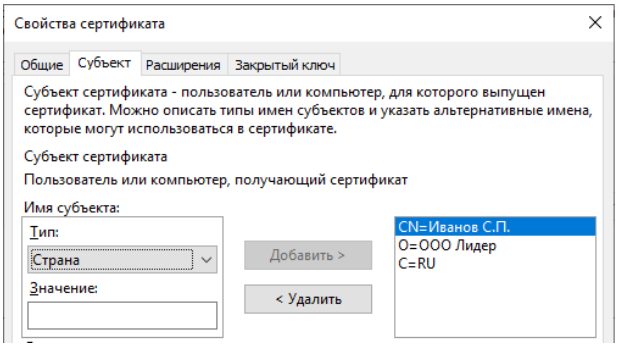
- «Понятное имя» - ФИО владельца ключа
- «Описание» - Наименование системы «NS-FiXit - » и наименование юридического лица, которому принадлежит ключ.



1.10. Перейти на закладку «Субъект» и заполнить данные о субъекте:

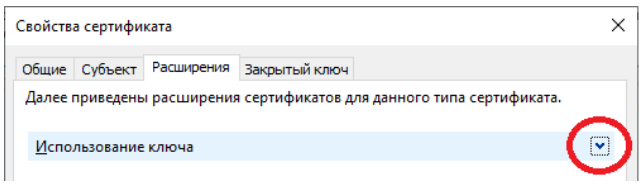
- «Общее имя» — Фамилия и инициалы физического лица – владельца подписи,
- «Организация» — Наименование организации без кавычек,
- «Страна» — двузначный код страны. Для резидентов «RU», для нерезидентов — в соответствии с Общероссийским классификатором стран мира (wikipedia).

В блоке «Имя субъекта» необходимо выбрать нужный тип параметра, ввести его значение и нажать кнопку «Добавить»:



В блоке «Дополнительное имя» ничего указывать не надо.

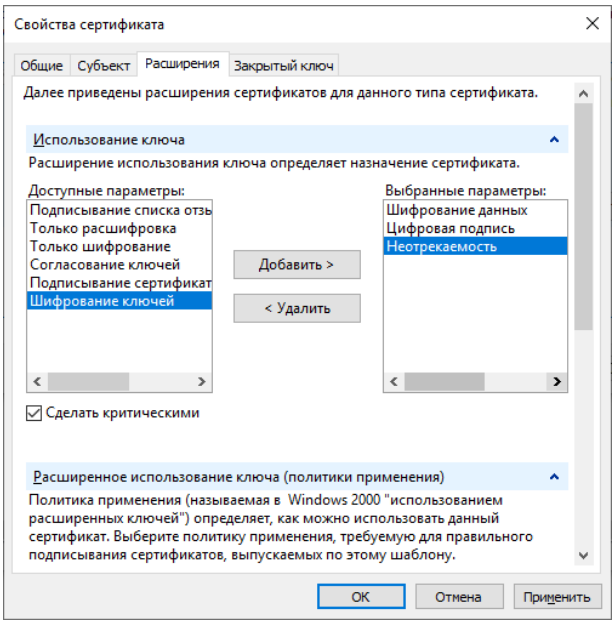
1.11. Перейти на закладку «Расширения» и раскрыть блок параметров «Использование ключа» нажатием на кнопку ⊡ в правой части строки:



1.12. Перенести из списка «Доступные параметры» в список «Выбранные параметры» следующие расширения ключа:

- Цифровая подпись
- Неотрекаемость
- Шифрование данных

Для этого надо выбрать параметр в списке доступных и нажать кнопку «Добавить»:

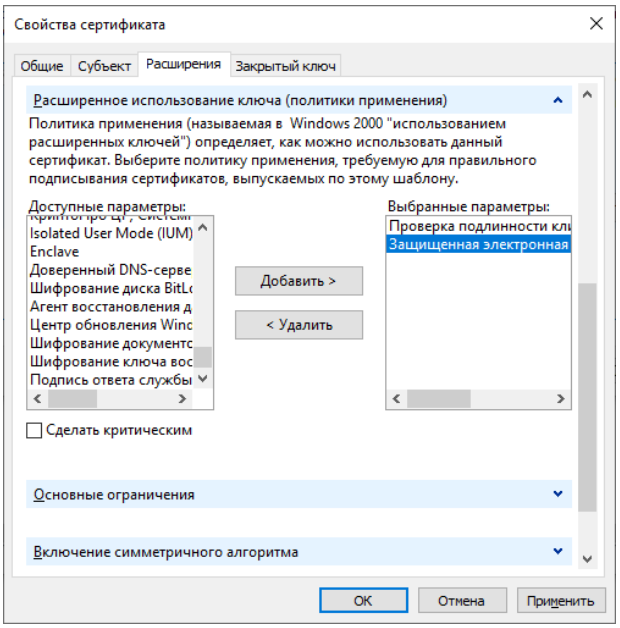


1.13. Раскрыть блок параметров «Расширенное использование ключа (политика применения)» нажатием на кнопку в правой части строки.

1.14. Перенести из списка «Доступные параметры» в список «Выбранные параметры» следующие расширения ключа:

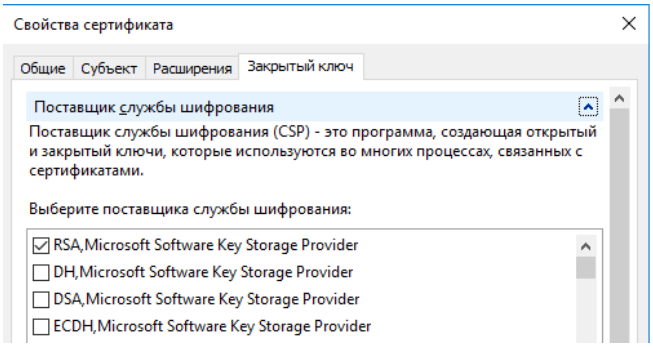
- Проверка подлинности клиента
- Защищенная электронная почта

Для этого надо выбрать параметр в списке доступных и нажать кнопку «Добавить»:



Остальные блоки менять не надо.

1.15. Перейти на закладку «Закрытый ключ» и раскрыть блок параметров «Поставщик службы шифрования» нажатием на кнопку в правой части строки. Убедитесь, что флаг установлен напротив «RSA, Microsoft Software Key Storage Provider»:

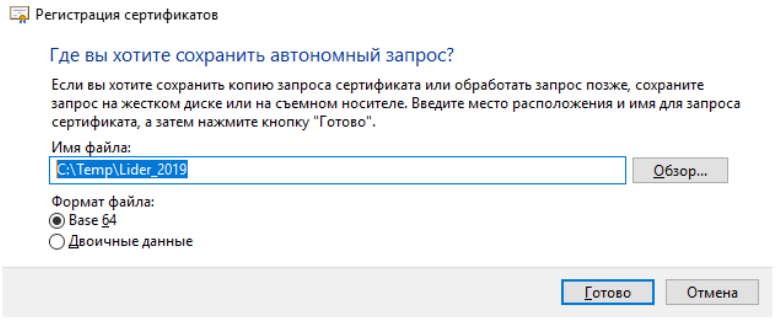


1.16. Раскрыть блок параметров «Параметры ключа» нажатием на кнопку в правой части строки и установить размер ключа 2048.

1.17. Установить флаги «Сделать закрытый ключ экспортируемым» и «Разрешить архивацию закрытого ключа».

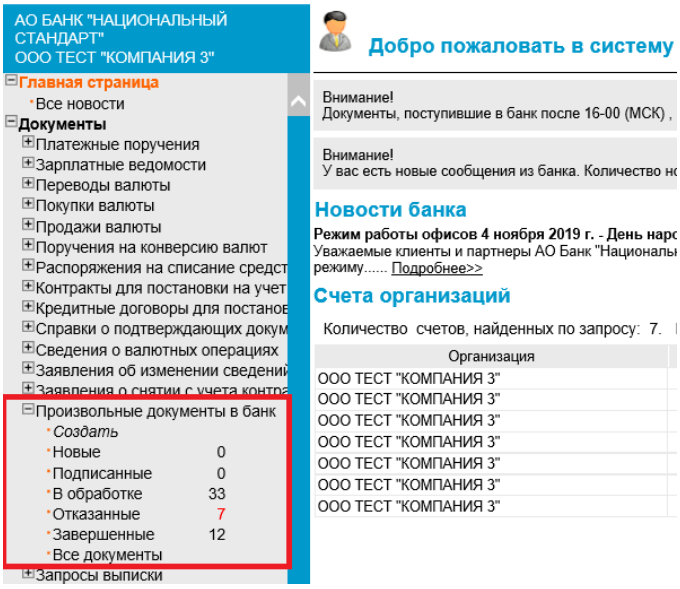
1.18. Остальные параметры менять не надо. Нажать Кнопку «ОК». Нажать кнопку «Далее».

1.19. Указать путь и имя файла для сохранения запроса на сертификат, установить кодировку «Base 64» и нажать «Готово»:



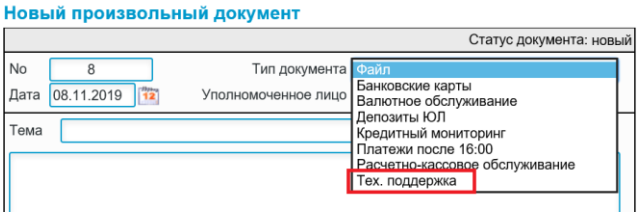
1.20. После этого в указанной папке сформируется файл запроса. Его необходимо отправить с помощью «Банк-Клиент» в банк.

1.21. В «Клиент-Банк» зайти в раздел «Произвольные документы в банк» и выбрать пункт «Создать»:



1.22. В письме указать:

- Тип: «Тех. поддержка»



- Тему: «NS-FiXit сертификат».
- Текст: «Просим выпустить сертификат по прилагаемому запросу».
- Прикрепить файл запроса, используя кнопку «Прикрепить новый файл».

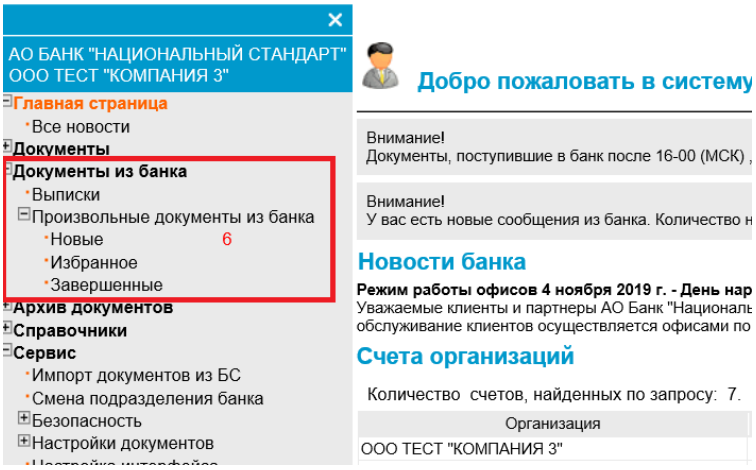
Важно!

Тип и тема письма обязательно должны быть такими, как указано выше. Иначе обработка документов будет произведена с задержкой по времени.

1.23. Отправить письмо в Банк.

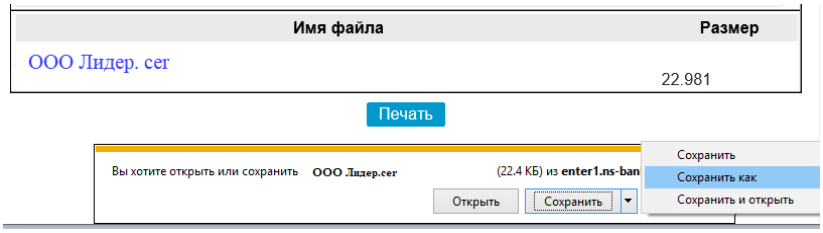
2. Получение сертификата и его установка

2.1. В ответ на полученный запрос на выпуск сертификата, Банк формирует клиентский сертификат и направляет его по системе Клиент-Банк. Для получения сертификата необходимо зайти в раздел «Документы из банка →Произвольные документы из банка» и выбрать пункт «Новые»:



2.2. Двойным кликом открыть письмо с темой «NS-FiXit сертификат». Письмо будет содержать два файла сертификатов: выпущенный на основании запроса клиентский сертификат и сертификат удостоверяющего центра Банка.

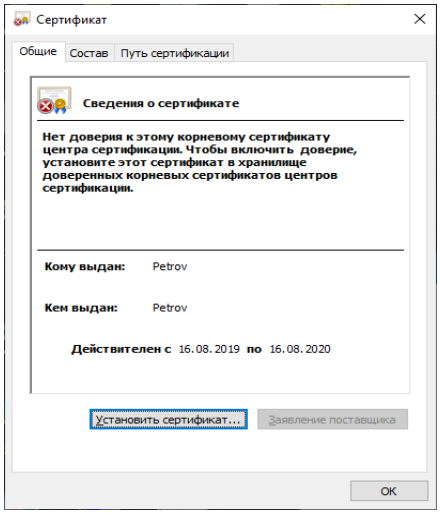
2.3. Левой кнопкой мышки щелкнуть по ссылке с именем файла. В открывшемся окне выбрать пункт «Сохранить как»:



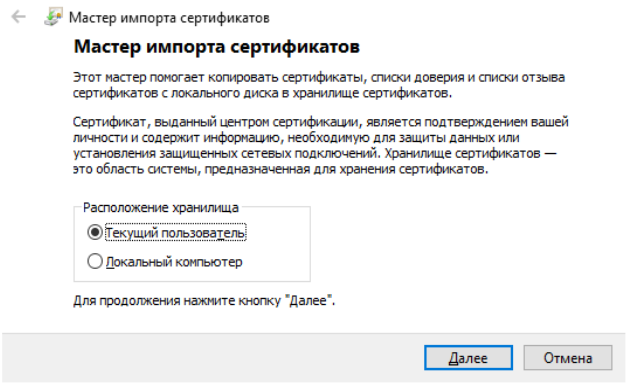
2.4. Сохранить файл сертификата в каталог, в котором будет удобно с ним работать.

2.5. Повторить операцию для обоих файлов.

2.6. Установить оба сертификата в систему. Для этого дважды щелкнуть мышкой по сохраненному файлу сертификата. Откроется окно информации о сертификате:



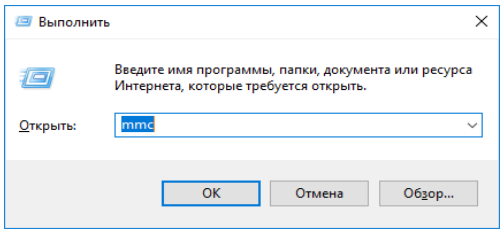
2.7. Нажать кнопку «Установить сертификат» — на экране откроется мастер импорта сертификатов:



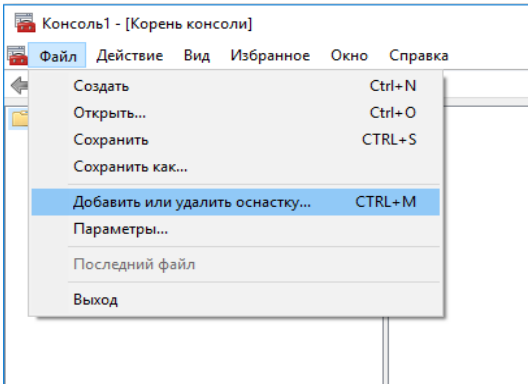
2.8. Нажать 2 раза кнопку «Далее» и кнопку «Готово».

2.9. Повторить операцию для второго сертификата.

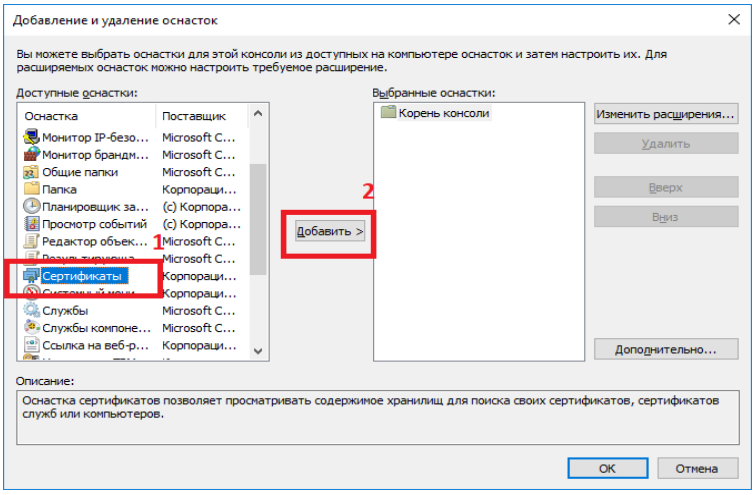
2.10. Запустить консоль управления Windows. Для этого щелкнуть правой кнопкой мышки по кнопке «Пуск» и выбрать пункт меню «Выполнить». В открывшемся окне набрать команду «mmc» и нажать кнопку «ОК»:



2.11. В открывшемся окне надо выбрать пункт меню «Файл → Добавить или удалить оснастку»:

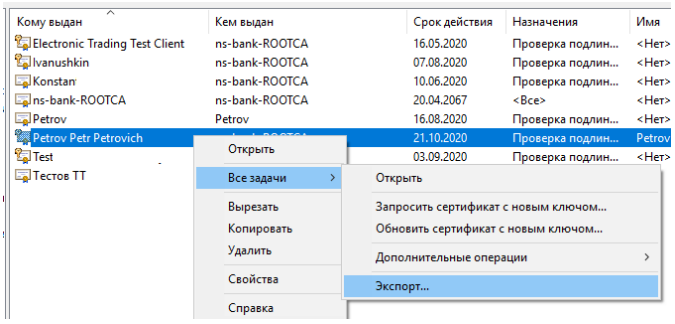


2.12. На экране откроется окно выбора оснастки. В левой части окна надо выбрать пункт «Сертификаты» и нажать кнопку «Добавить»:



2.13. В левой части консоли выбрать раздел «Личное».

2.14. Необходимо выбрать в списке свой сертификат. Щелкнуть по нему правой кнопкой мышки и выбрать пункт меню «Все задачи → Экспорт»:



2.15. В открывшемся окне мастера экспорта сертификатов нажать кнопку «Далее».

2.16. На следующем шаге установить флаг «Да, экспортировать закрытый ключ» и нажать кнопку «Далее».

2.17. На следующем шаге установить флаг «Включить по возможности все сертификаты в пути сертификации» и «Включить конфиденциальность сертификата» и нажать кнопку «Далее».

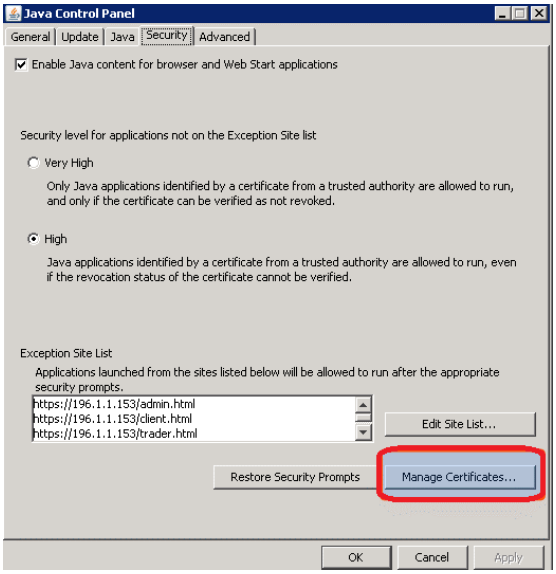
2.18. На шаге «Безопасность» необходимо установить пароль на экспортированный ключ. Пароль необходимо запомнить, он будет использоваться в дальнейшем при доступе на сайт услуги «NS-FiXit».

Пароль должен быть длиной не менее 10 символов и содержать заглавные и прописные латинские буквы и цифры (рекомендуется также использовать спец. символов — ~!@#$ и п.р.).

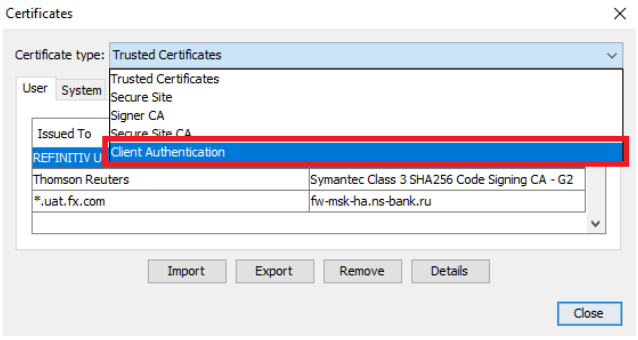
2.19. После ввода пароля надо нажать кнопку «Далее».

2.20. На следующем шаге надо указать каталог, в котором будет удобно работать с файлом сертификата, и имя файла. Нажать кнопку «Далее». Нажать кнопку «Готово».

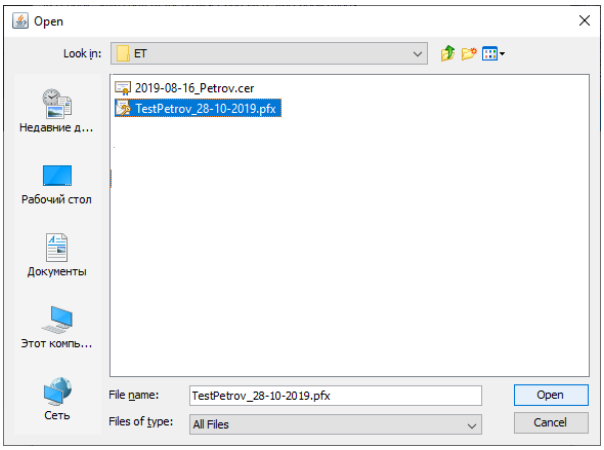
2.21. Открыть настройки Java: «Пуск → Программы → Java → Configure Java», перейти на закладку «Security» и нажать кнопку «Manage Certificates…»:



2.22. В открывшемся окне указать тип сертификата (Certificate type): «Client Authentication» и нажать кнопку «Import»:

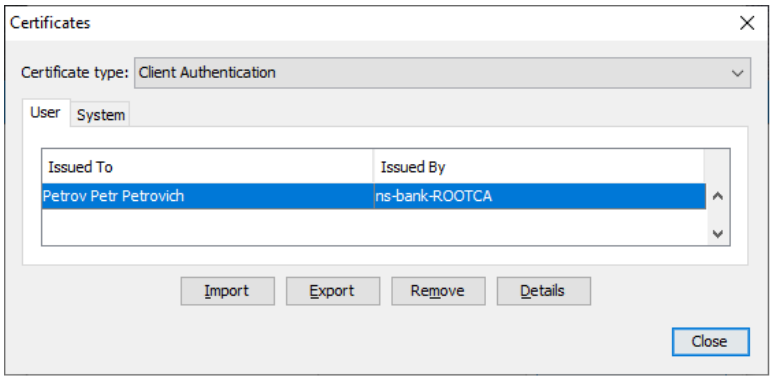


2.23. В открывшемся окне выбрать тип файлов (Files of type) – All files. Указать файл сертификата с расширением pfx, экспорт которого описан в пунктах 2.16 -2.23 данной инструкции:



2.24. Java запросит ввод пароля. Ввести пароль, указанный на шаге 2.20 данной инструкции.

2.25. После импорта появится строчка с записью об импортированном сертификате, после чего можно закрыть окно настроек Java:



2.26. Все необходимые настройки выполнены — можно работать в системе.