

СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

**Пособие по настройке сертификатов электронной
подписи на рабочем месте пользователя**

Оглавление

ВВЕДЕНИЕ.....	3
ПЕРЕД ТЕМ КАК НАЧАТЬ.....	4
КАК ПОЛУЧИТЬ ФАЙЛ ЭКСПОРТА СЕРТИФИКАТА.....	4
КАК ОПРЕДЕЛИТЬ, КАКАЯ ДОЛЖНА БЫТЬ «ЦЕПОЧКА» СЕРТИФИКАТОВ.....	7
КАК УСТАНОВИТЬ «ЦЕПОЧКУ» СЕРТИФИКАТОВ НА КОМПЬЮТЕРЕ.....	10
УСТАНОВКА ЛИЧНОГО СЕРТИФИКАТА.....	10
УСТАНОВКА ПРОМЕЖУТОЧНЫХ СЕРТИФИКАТОВ.....	10
УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА.....	15
КАК ПРОВЕРИТЬ ПРАВИЛЬНОСТЬ УСТАНОВКИ «ЦЕПОЧКИ» СЕРТИФИКАТОВ	17



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

Введение

Настоящий документ представляет собой пособие по выполнению необходимых действий для настройки сертификатов электронной подписи для использования в системе электронной подачи заявок на изобретения и полезные модели (далее - Сервис подачи).

В Сервисе для авторизации пользователя и подписывания электронных заявок используются *только* личные сертификаты квалифицированной электронной подписи, выдаваемые аккредитованными при Министерстве связи и массовых коммуникаций Российской Федерации Удостоверяющими центрами (далее – Сертификат) по ГОСТ Р 34.11/34.10-2001 и ГОСТ Р 34.11-2012/34.10-2012 256 бит.

Правильно установленный сертификат должен образовывать т.н. «цепочку» сертификатов – корневой сертификат, промежуточный сертификат и, наконец, личный Сертификат.

Далее, на примере тестового сертификата, выпущенного Удостоверяющим центром Федерального института промышленной собственности, будут последовательно рассмотрены шаги по выстраиванию этой «цепочки» на компьютере пользователя.

Обратите внимание, что этот сертификат и все остальные, упомянутые в данном пособии использованы только в качестве учебного примера. Вы должны проделать операции, здесь перечисленные с Вашим личным сертификатом.



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

Перед тем как начать

Прежде чем начать, убедитесь, что у Вас есть:

1. Полученный в аккредитованном Удостоверяющем центре¹ личный Сертификат ЭП на электронном носителе (eToken, ruToken или др.).
2. Установленное на Вашем компьютере программное обеспечение Крипто-ПРО CSP версии не ниже 4.0 или иной криптопровайдер².
3. Файл экспорта Вашего Сертификата в колировке DER или BASE64 (если Вы знаете, как получить файл экспорта сертификата, можете пропустить следующий раздел и перейти к разделу «Как определить, какая должна быть «цепочка» сертификатов»).

Как получить файл экспорта Сертификата

Важно! *Получить файл экспорта Сертификата можно только после его установки на Ваш компьютер. Чтобы установить личный сертификат с закрытым ключом используйте Ваш криптопровайдер. Пошаговая инструкция по установке личного ключа находится в пользовательской документации криптопровайдера.*

Чтобы получить файл экспорта установленного² личного сертификата следует выполнить следующие действия:

1. В меню «Пуск» Windows в строке поиска наберите `certmgr.msc`. Откроется окно консоли сертификатов «certmgr - [Сертификаты - текущий пользователь]».

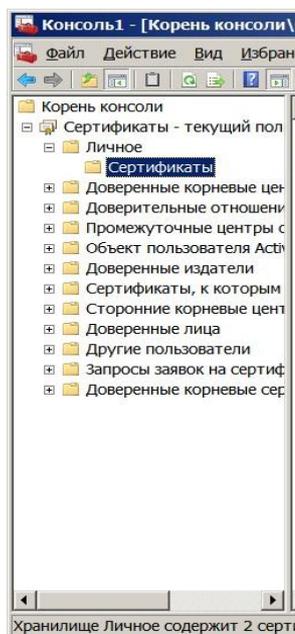
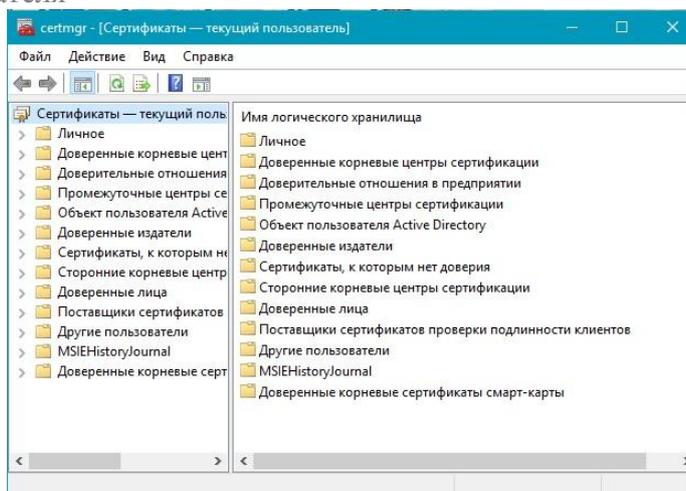
¹ Список аккредитованных Удостоверяющих центров опубликован в сети Интернет по адресу <http://e-trust.gosuslugi.ru/CA>.

² Более подробно об установке программного обеспечения криптопровайдера см. документацию разработчика Вашего криптопровайдера.

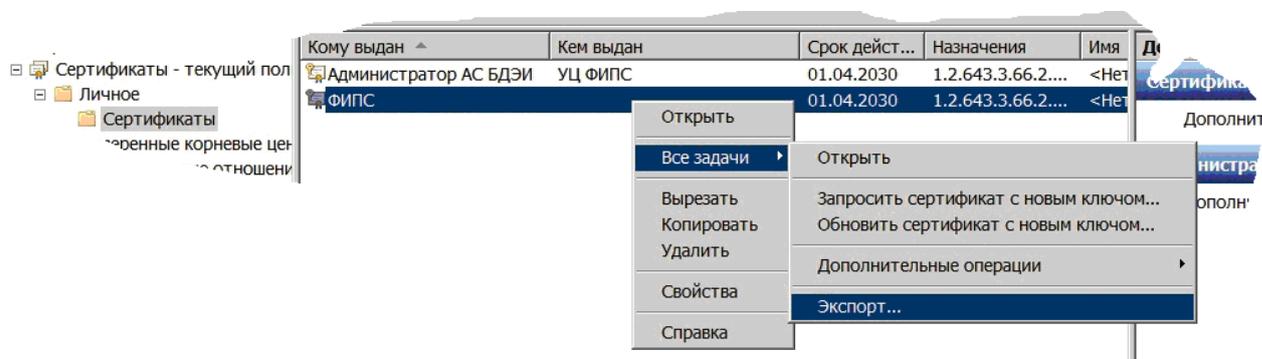


СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя



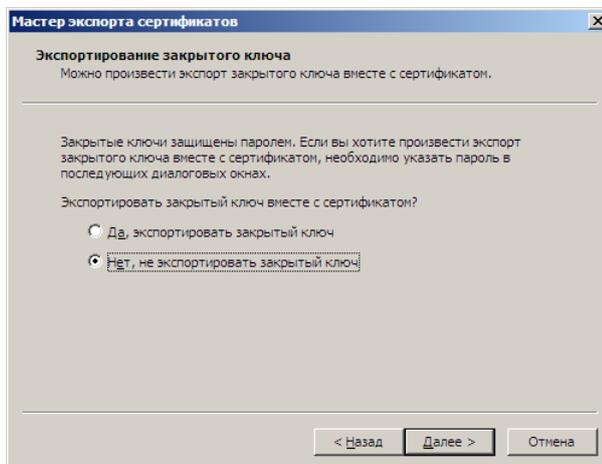
2. В окне консоли сертификатов в дереве слева выберите, как показано на рисунке слева «Сертификаты - текущий пользователь» - «Личное» - «Сертификаты».
3. Выберите в списке справа Ваш личный Сертификат и щелкните на нем правой кнопкой мыши. В открывшемся контекстном меню выберите пункт «Все задачи...» и в нем – «Экспорт...», как показано на рисунке ниже.



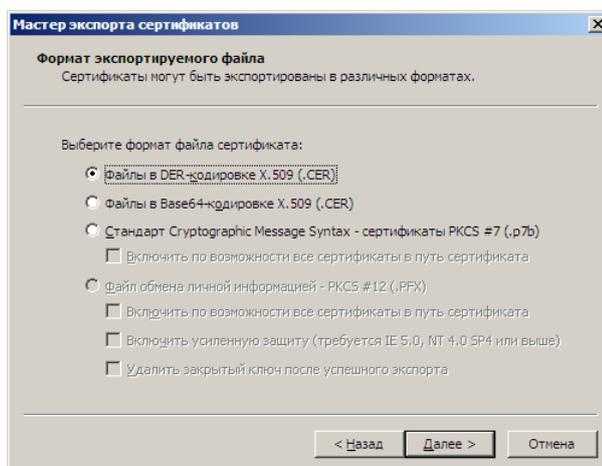
4. Откроется окно «Мастер экспорта сертификатов». На первой странице («Вас приветствует мастер сертификатов») нажмите кнопку «Далее».



5. На странице «Экспортирование закрытого ключа» выберите радиокнопку «Нет, не экспортировать закрытый ключ» и нажмите кнопку «Далее».



6. На странице «Формат экспортируемого файла» выберите один из двух форматов (Файлы в DER-кодировке X.509 или Файлы в Base64-кодировке X.509) и нажмите кнопку «Далее».

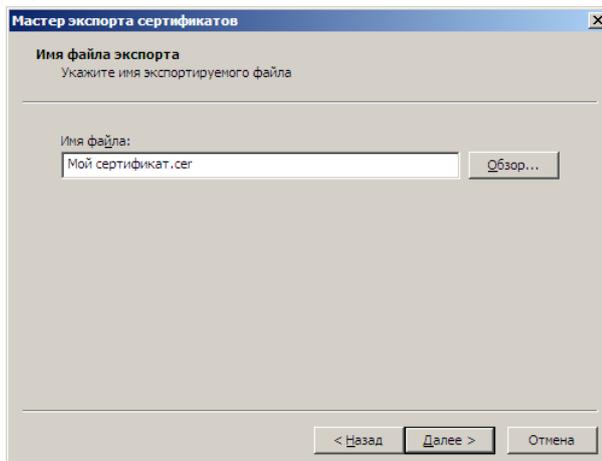


7. На странице «Имя файла экспорта» укажите имя файла, например, Мой сертификат.cer, или воспользуйтесь кнопкой «Обзор» для указания местоположения и имени файла экспорта и нажмите кнопку «Далее».



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя



8. На странице «Завершение работы мастера сертификатов» нажмите кнопку «Готово», потом кнопку «ОК».
9. Закройте окно «certmgr - [Сертификаты - текущий пользователь]». Файл экспорта Сертификата создан.

Как определить, какая должна быть «цепочка» сертификатов

* Выберите сертификат для проверки:

Загрузить файл...

* Введите код на изображении:

52497

▶ Проверить

Чтобы определить, какие сертификаты (корневой сертификат и промежуточные сертификаты) вместе с личным сертификатом будут образовывать правильную «цепочку», надо проверить Ваш личный Сертификат на Портале Госуслуг (<http://www.gosuslugi.ru/pgu/eds>). На странице «Подтверждение подлинности ЭП сертификата»

загрузите созданный Вами файл экспорта (см. раздел «Как получить файл экспорта Сертификата»), введите код на изображении и нажмите кнопку «Проверить».

Результат проверки будет отображен на странице (см. рисунок ниже). Давайте разберем картинку. В первую очередь надо обратить внимание на область, выделенную на рисунке ниже, синей границей. Если там содержатся слова «ДЕЙСТВИТЕЛЕН» и «сертификат выдан аккредитованным удостоверяющим центром», значит все в порядке, Ваш сертификат может использоваться для работы с сервисом подачи. Если же каких-либо из этих слов нет, значит с Вашим сертификатом далее работать не имеет смысла, и Вам надо получать новый.



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

Теперь разберем «цепочку». «Цепочка» строится от личного сертификата через промежуточные сертификаты до корневого. Сколько сертификатов составляют «цепочку»? Столько, сколько строк «Действителен» на странице. «Цепочка» строится сверху вниз - первый всегда личный сертификат, последний - всегда корневой. Между ними располагаются промежуточные сертификаты (в данном случае один). На картинке сведения о сертификатах, составляющих «цепочку», выделены красными прямоугольниками с номерами от 1 до 3.

Первая выделенная область (номер 1) содержит сведения о Вашем личном сертификате. Нас интересует строка «Издатель». Текст до первой запятой после слова «Издатель:» - это название удостоверяющего центра, выпустившего Ваш личный сертификат и одновременно - название промежуточного сертификата, следующего сразу за личным в «цепочке». Теперь смотрим, кем выдан этот промежуточный сертификат. Сведения об этом содержатся в области, помеченной номером 2. Смотрим строку «Издатель». В ней значится «Минкомсвязь России». Это следующий сертификат в «цепочке». Какой он - промежуточный или корневой? Смотрим следующую область (номер 3)? строку «Издатель». Здесь снова «Минкомсвязь России». Значит, этот сертификат выдан «самим собой», т.е. «самоподписанным», или корневым. «Цепочка» завершена.



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

Проверка выполнена

Подлинность сертификата ПОДТВЕРЖДЕНА

Статус сертификата, использованного для подтверждения подлинности ЭП: ДЕЙСТВИТЕЛЕН, сертификат выдан аккредитованным удостоверяющим центром

Статусы использованных сертификатов

Владелец ФИПС: [REDACTED] RU, 77 Москва, Москва, ФИПС [REDACTED]

Издатель: Федеральный институт промышленной собственности, Федеральный институт промышленной собственности, Бережковская набережная д. 30 к.1, Москва, 77 Москва, RU, 007730036073, 1027739154343, fipsca@rupto.ru

Действителен: с 2018.08.10 по 2033.07.27 **1**

Уполномоченное лицо УЦ: Федеральный институт промышленной собственности, Федеральный институт промышленной собственности, Бережковская набережная д. 30 к.1, Москва, 77 Москва, RU, 007730036073, 1027739154343, fipsca@rupto.ru

Издатель: Минкомсвязь России, 007710474375, 1047702026701, Минкомсвязь России, "улица Тверская, дом 7", г. Москва, 77 Москва, RU, dit@minsvyaz.ru

Действителен: с 2018.07.27 по 2033.07.27 **2**

Уполномоченное лицо УЦ: Минкомсвязь России, 007710474375, 1047702026701, Минкомсвязь России, "улица Тверская, дом 7", г. Москва, 77 Москва, RU, dit@minsvyaz.ru

Издатель: Минкомсвязь России, 007710474375, 1047702026701, Минкомсвязь России, "улица Тверская, дом 7", г. Москва, 77 Москва, RU, dit@minsvyaz.ru

Действителен: с 2018.07.06 по 2036.07.01 **3**

Таким образом, наша «цепочка» состоит из трех сертификатов:

Личный сертификат с названием «ФИПС³» - промежуточный сертификат «Федеральный институт промышленной собственности⁴» - корневой сертификат «Минкомсвязь России⁵»

³ В Вашем конкретном случае здесь будет Ваше ФИО или название Вашей организации. «ФИПС» - только для примера!

⁴ В Вашем конкретном случае здесь будет название удостоверяющего центра, выдавшего Ваш личный сертификат.

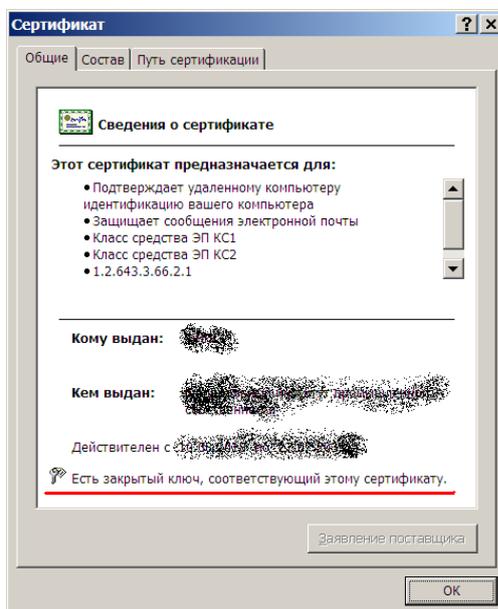
⁵ Если Ваш личный сертификат соответствует стандарту ГОСТ Р 34.11-2012/34.10-2012 256 бит, здесь будет «Минкомсвязь России». Если же он соответствует стандарту ГОСТ Р 34.11/34.10-2001, здесь будет «Головной удостоверяющий центр». Чтобы узнать, какому стандарту соответствует Ваш сертификат, откройте его (двойным щелчком) из сохраненного Вами ранее файла экспорта сертификата (см. Как получить файл экспорта Сертификата), перейдите на закладку «Состав» и выберите строку «Алгоритм подписи».



Как установить «цепочку» сертификатов на компьютере

Установка личного сертификата

Процесс установки личного сертификата с закрытым ключом описан в пользовательской документации программного обеспечения криптопровайдера, установленного на Вашем компьютере (см. «Перед тем как начать»). В результате установки открытый в консоли сертификат должен выглядеть так.



Самое главное, что была строчка, подчеркнутая на рисунке выше красной линией.

Установка промежуточных сертификатов

Найти его можно в сети Интернет на Портале уполномоченного федерального органа в области использования электронной подписи по адресу

<http://e-trust.gosuslugi.ru/CA>.

СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ



Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

Портал уполномоченного федерального органа в области использования электронной подписи

Вход для аккредитованных УЦ
Вход через ЕСИА

ГЛАВНАЯ АККРЕДИТАЦИЯ ГОЛОВНОЙ УЦ РЕЕСТРЫ ОБЪЕКТНЫЕ ИДЕНТИФИКАТОРЫ РФ

МОНИТОРИНГ УЦ НОРМАТИВНЫЕ ДОКУМЕНТЫ КОНТАКТЫ

Данный раздел содержит перечень аккредитованных удостоверяющих центров

Скачать XML-представление
Головной удостоверяющий центр
УЦ на карте

Фильтр

Название: ОГРН: Псевдоним ПАК: Статус аккредитации:
Федеральный институт промышл -- Все --

Город: Средства УЦ: Класс средств ЭП:
-- Все -- -- Все -- -- Все --

Применить Сбросить

1. В поле «Псевдоним ПАК» (на рисунке выше - 1) вводим название промежуточного сертификата «Федеральный институт промышленной собственности⁶» и нажимаем кнопку «Применить» (на рисунке выше - 2).
2. Если название введено правильно, на странице появится ссылка на информацию об Удостоверяющем центре. Щелкните по изображению увеличительного стекла слева от названия удостоверяющего центра (на рисунке ниже обведено красным). Откроется страница сведений об удостоверяющем центре.

Всего записей: 1. Страницы: 1

Наименование УЦ	Город	Статус
 Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	Москва	Действует

3. Найдите на странице информацию о нужном ПАКе (название пака совпадает с названием сертификата). Под названием ПАКа может быть несколько сертификатов или на странице может находиться несколько одинаковых названий ПАК. Чтобы выбрать нужный, сделайте следующее.
 - Откройте файл экспорта сертификата (см. Как получить файл экспорта Сертификата) и перейдите на закладку «Состав».
 - Выберите строку «Идентификатор ключа центра сертификатов». В нижней части окна сертификата (см. рисунок ниже) найдите строку «Идентификатор

⁶ В вашем конкретном случае будет название удостоверяющего центра, выдавшего Ваш личный сертификат.



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

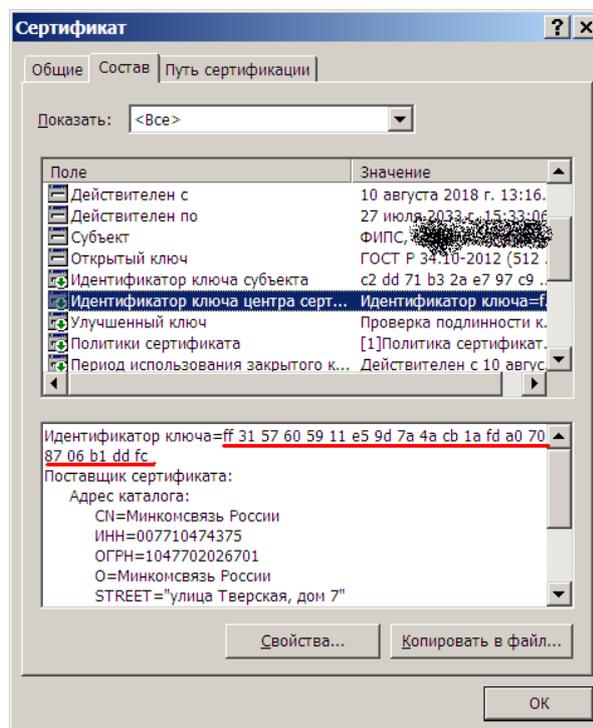
Пособие по настройке сертификатов электронной подписи на
рабочем месте пользователя

ключа=...». Скопируйте часть строки после знака «=» куда-нибудь и удалите
пробелы. Например, так: ff3157605911e59d7a4acb1afda0708706b1ddfc.

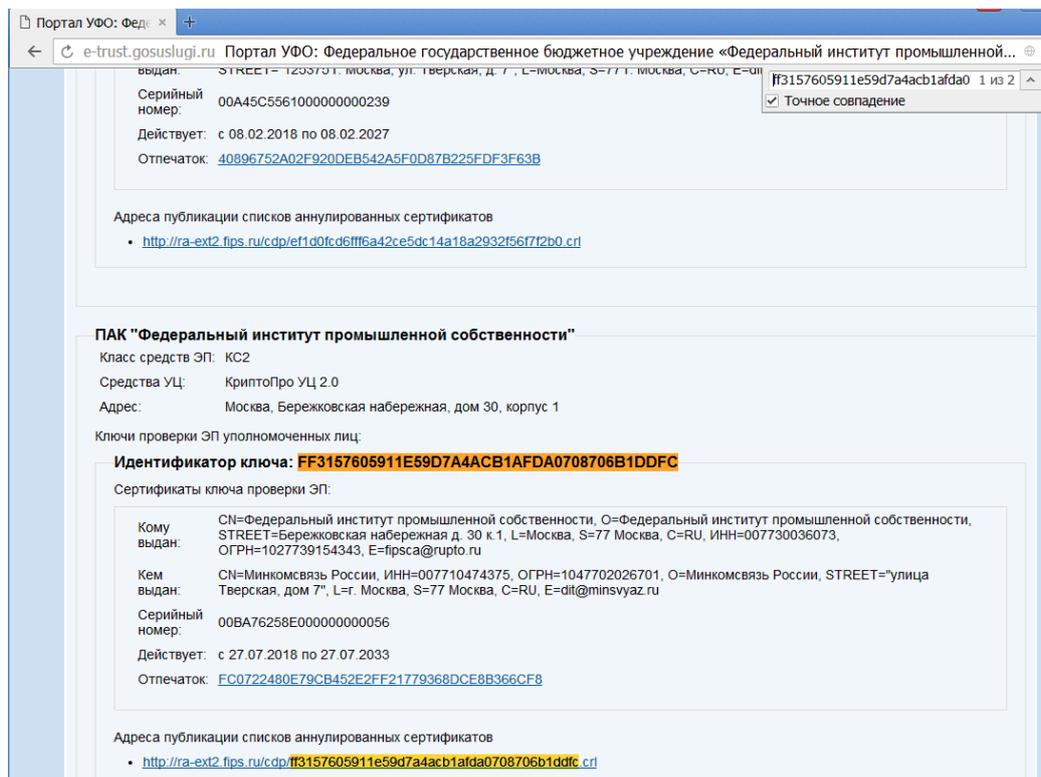


СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

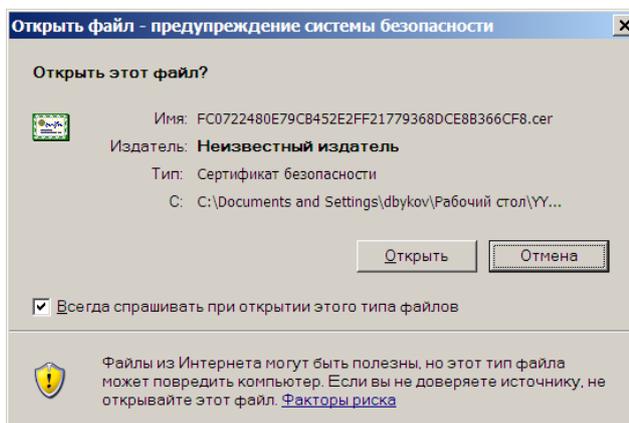


Теперь на странице ПАК найдите строку «Идентификатор ключа:... » с таким же значением. Можно воспользоваться комбинацией клавиш Ctrl-F, как на рисунке ниже.

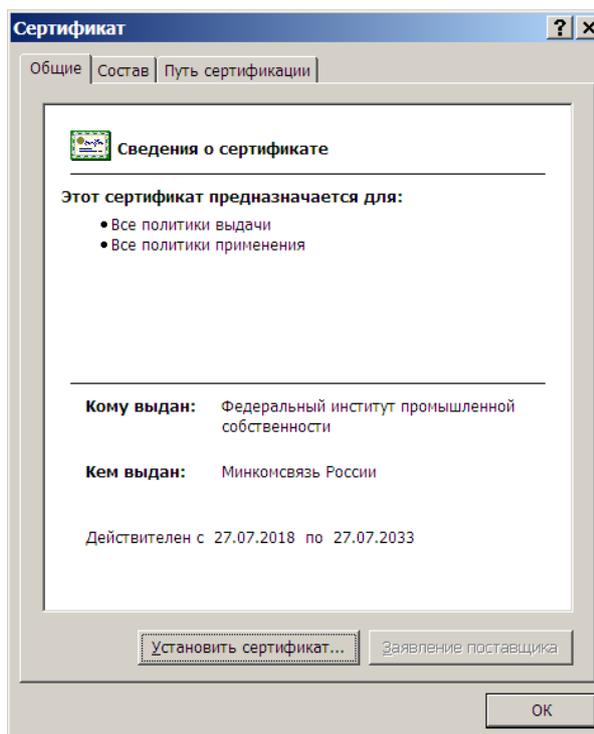




4. Вам нужна ссылка «Отпечаток». Щелкните по ней и сохраните куда-нибудь файл промежуточного сертификата.
5. Откройте сохраненный файл промежуточного сертификата.



6. Нажмите кнопку «Открыть».

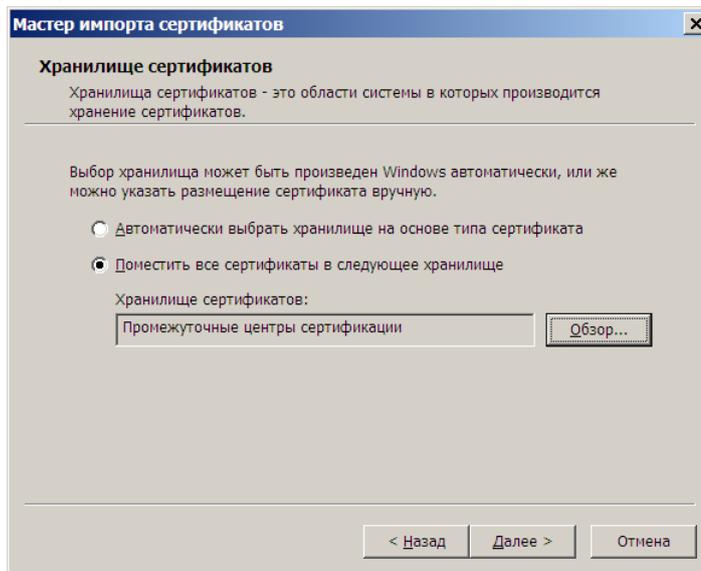


7. Нажмите кнопку «Установить сертификат».
8. Откроется окно «Мастер импорта сертификатов». На странице «Вас приветствует мастер импорта сертификатов» нажмите кнопку «Далее».
9. На странице «Хранилище сертификатов» выберите «Поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и выберите «Промежуточные центры сертификации».



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя



Нажмите кнопку «Далее».

10. На странице «Завершение работы мастера импорта сертификатов» нажмите кнопку «Готово», и в окне «Импорт успешно выполнен» кнопку «ОК».
11. Установка промежуточного сертификата завершена.
12. Если в «цепочке» Вашего личного сертификата есть ещё промежуточные сертификаты (см. Как определить, какая должна быть «цепочка» сертификатов»), повторите действия этого раздела для них, только значение «Идентификатор ключа» для поиска нужного сертификата на странице ПАК (см. п. 3 этого раздела) ищите не в личном сертификате, а в только что установленном промежуточном.
13. Если промежуточных сертификатов в «цепочке» больше нет, переходите к следующему разделу.

Установка корневого сертификата

Корневым (и последним в «цепочке») является сертификат «Минкомсвязь России⁷». Найти его можно в сети Интернет на Портале уполномоченного федерального органа в области использования электронной подписи по адресу <http://e-trust.gosuslugi.ru/MainCA>. Чтобы скачать сертификат, найдите на странице ПАК с названием «Минкомсвязь России». Их может оказаться несколько. Для выбора нужного откройте последний установленный промежуточный сертификат и на закладке «Состав» в

⁷ Если Ваш личный сертификат соответствует стандарту ГОСТ Р 34.11-2012/34.10-2012 256 бит, здесь будет «Минкомсвязь России». Если же он соответствует стандарту ГОСТ Р 34.11/34.10-2001, здесь будет «Головной удостоверяющий центр».



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

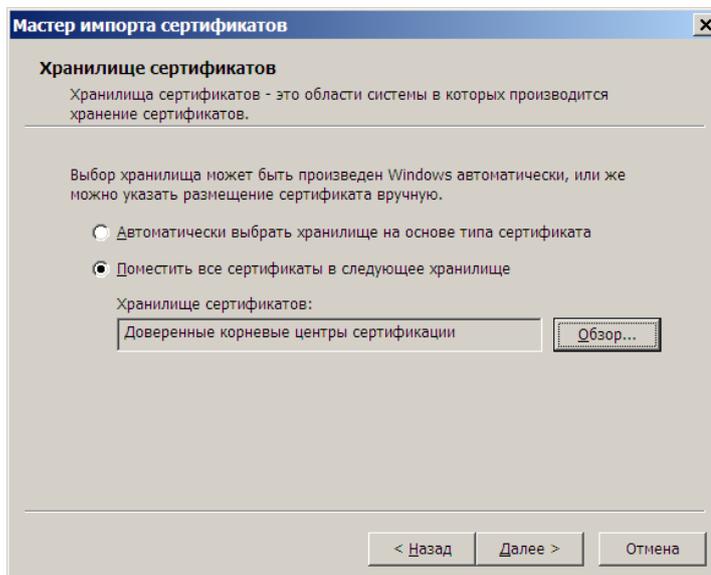
Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

строке «Идентификатор ключа центра сертификатов» найдите и скопируйте значение «Идентификатор ключа» (так же, как это Вы делали в п. 3 раздела Установка промежуточных сертификатов)



2. Вам нужна ссылка «Отпечаток». Щелкните по ней и сохраните куда-нибудь файл корневого сертификата.

3. Далее установите корневой сертификат на Ваш компьютер. Делается это точно так же, как и при установке промежуточных сертификатов (см. пункты 5-10 раздела Установка промежуточных сертификатов), только при выборе хранилища сертификата (пункт 9 раздела Установка промежуточных сертификатов) укажите «Доверенные корневые центры сертификации»



4. На этом установка «цепочки» сертификатов завершена.



СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

Пособие по настройке сертификатов электронной подписи на рабочем месте пользователя

Как проверить правильность установки «цепочки» сертификатов

Чтобы проверить правильность вышеперечисленных действий, снова откройте консоль управления сертификатами, как описано в разделе «Как получить файл экспорта Сертификата». Найдите в «Сертификаты - текущий пользователь»-«Сертификаты»-«Личное» Ваш личный сертификат и откройте его двойным щелчком левой кнопки мыши. В открывшемся сертификате перейдите на закладку «Путь сертификации».

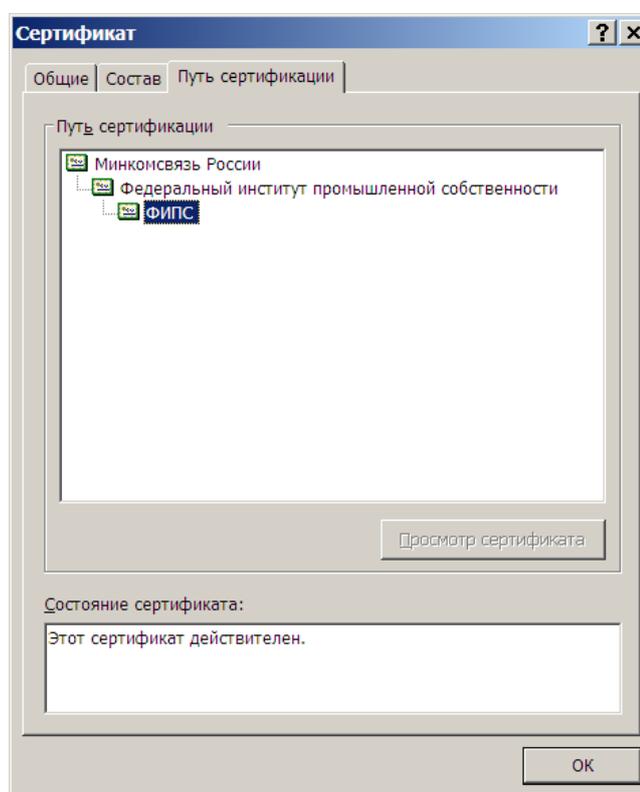


Рисунок 1

Если все сертификаты установлены правильно, закладка «Путь сертификации» должна выглядеть так, как показано на рисунке выше. В Вашем конкретном случае названия сертификатов могут быть другими, но «цепочка» должна начинаться (снизу) Вашим личным сертификатом и заканчиваться (вверху) корневым сертификатом - «Минкомсвязь России» или «Головной удостоверяющий центр». Значки сертификатов «цепочки» должны быть такими , а не такими !