Руководство по установке квалифицированного сертификата ЭП, выданного аккредитованным Удостоверяющим центром

Москва, 2013

Оглавление

1. Используема терминология

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи (далее – **квалифицированный сертификат**) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона.

Аутентификация – процедура проверки подлинности данных и субъектов информационного взаимодействия исключительно на основе внутренней структуры самих данных.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной

подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Открытый ключ ЭП – криптографический ключ, который связан с секретным (закрытым, личным) ключом специальным математическим соотношением. Открытый ключ известен всем пользователям системы и предназначен для проверки ЭП.

Открытый ключ электронно-цифровой подписи (по законодательству РФ) – уникальная последовательность символов:

- соответствующая закрытому ключу электронной цифровой подписи;
- доступная любому пользователю информационной системы;
- предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Открытый ключ позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить секретный ключ.

Закрытый ключ ЭП (по законодательству РФ) – уникальная последовательность символов:

- известная владельцу сертификата ключа подписи;
- предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

2. Введение

Настоящий документ содержит требования и инструкции установки сертификата электронной подписи для использования в системе электронной подачи заявок на регистрацию товарного знака и знака обслуживания (далее – КПС РТЗ).

В КПС РТЗ для аутентификации пользователя и подачи электронных документов используются квалифицированные сертификаты электронной подписи, выдаваемые аккредитованными при Министерстве связи и массовых коммуникаций Российской Федерации Удостоверяющими центрами (далее – Сертификат).

Правильно установленный сертификат должен обеспечить проверку «цепочки доверия» сертификатов, состоящую из корневого сертификата, кросс-сертификата верхнего уровня, кросс-сертификата Вашего Удостоверяющего центра и личного Сертификата.

3. Действия перед установкой Сертификата

Прежде чем начать установку Сертификата, убедитесь, что у Вас есть:

1. Полученный в аккредитованном Удостоверяющем центре[1] личный Сертификат ЭП на электронном носителе (eToken или ruToken).

2. Установленное на Вашем компьютере программное обеспечение Крипто-ПРО CSP или иные средства электронной подписи[2].

3. Файл с Вашим Сертификатом в колировке DER или BASE64[3].

4. Определение «цепочки» сертификатов

Для того чтобы определить нужные сертификаты (корневой и кросс-сертификаты), следует проверить Ваш личный Сертификат на Портале Госуслуг по адресу www.gosuslugi.ru/pgu/eds. На странице «Подтверждение подлинности ЭП сертификата» загрузите созданный Вами файл Сертификата, введите код на изображении и нажмите кнопку «Проверить» (см. Рисунок 1).

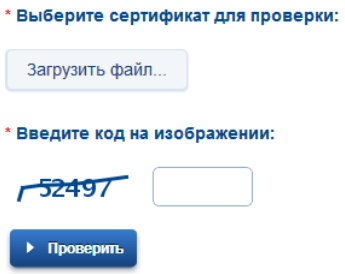


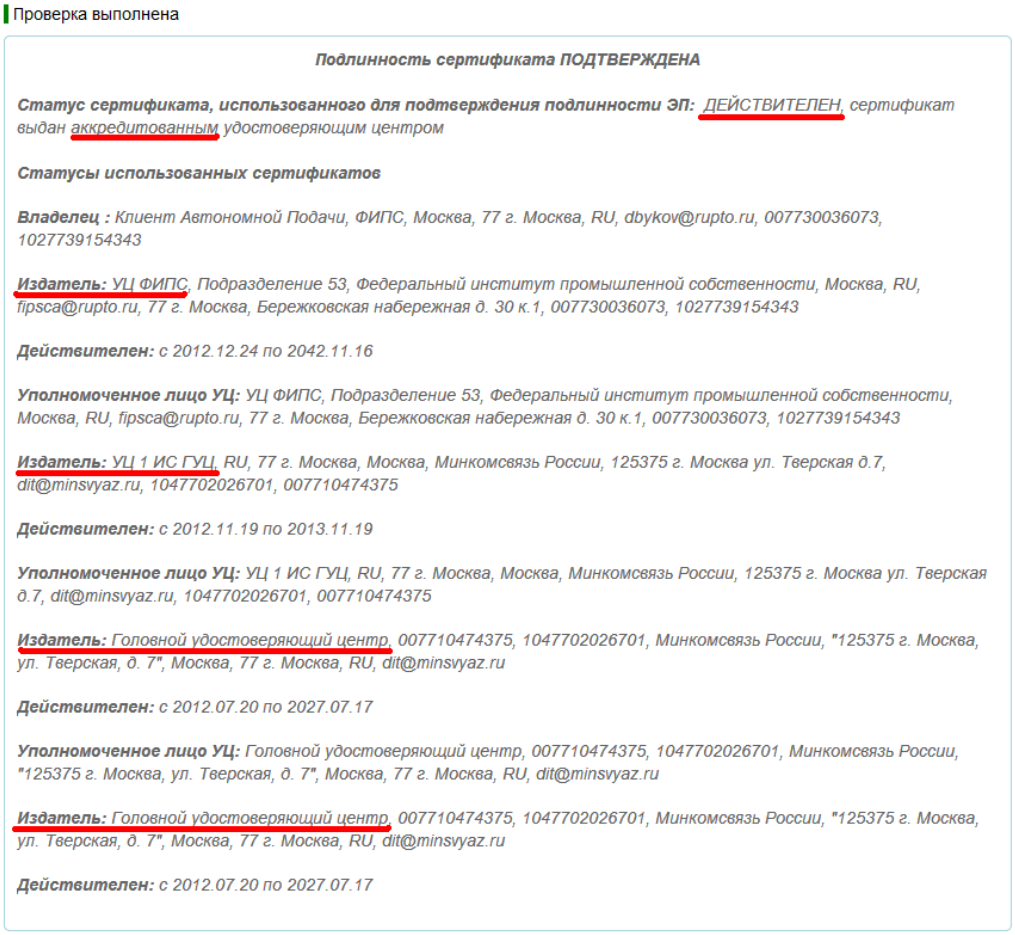
Рисунок 1

[1] Список аккредитованных Удостоверяющих центров опубликован в сети Интернет по адресу e-trust.gosuslugi.ru/CA.

[2] Более подробно об установке средств электронной подписи см. документ «Инструкция по установке КриптоПро версии 3.6, корневого и личного сертификатов» в сети Интернет по адресу http://www1.fips.ru/file_site/instruct_CSP_3.6.pdf.

[3] Более подробно об экспорте личного Сертификата см. документ «Экспорт сертификата открытого ключа в браузере Internet Explorer» в сети Интернет по адресу www1.fips.ru/file_site/instr_exp_kee.pdf.

Результат проверки будет отображен на странице (см. Рисунок 2). Здесь важна следующая информация: сертификат *действителен* и выдан *аккредитованным* удостоверяющим центром.


Проверка выполнена

Подлинность сертификата ПОДТВЕРЖДЕНА

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

Статусы использованных сертификатов

Владелец : *Клиент Автономной Подачи, ФИПС, Москва, 77 г. Москва, RU, dbykov@rupto.ru, 007730036073, 1027739154343*

Издатель: *УЦ ФИПС, Подразделение 53, Федеральный институт промышленной собственности, Москва, RU, fipsca@rupto.ru, 77 г. Москва, Бережковская набережная д. 30 к.1, 007730036073, 1027739154343*

Действителен: *с 2012.12.24 по 2042.11.16*

Уполномоченное лицо УЦ: *УЦ ФИПС, Подразделение 53, Федеральный институт промышленной собственности, Москва, RU, fipsca@rupto.ru, 77 г. Москва, Бережковская набережная д. 30 к.1, 007730036073, 1027739154343*

Издатель: *УЦ 1 ИС ГУЦ, RU, 77 г. Москва, Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru, 1047702026701, 007710474375*

Действителен: *с 2012.11.19 по 2013.11.19*

Уполномоченное лицо УЦ: *УЦ 1 ИС ГУЦ, RU, 77 г. Москва, Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru, 1047702026701, 007710474375*

Издатель: *Головной удостоверяющий центр, 007710474375, 1047702026701, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru*

Действителен: *с 2012.07.20 по 2027.07.17*

Уполномоченное лицо УЦ: *Головной удостоверяющий центр, 007710474375, 1047702026701, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru*

Издатель: *Головной удостоверяющий центр, 007710474375, 1047702026701, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru*

Действителен: *с 2012.07.20 по 2027.07.17*

Рисунок 2

Теперь, чтобы определить цепочку сертификатов, ищите слова «Издатель» - сверху вниз:

«Издатель: УЦ ФИПС» – это кросс-сертификат Вашего Удостоверяющего центра,

«Издатель: УЦ 1 ИС ГУЦ» - это кросс-сертификат верхнего уровня,

«Издатель: Головной удостоверяющий центр» - это корневой сертификат.

5. Установка корневого сертификата

Корневым для Сертификатов, выданных аккредитованным Удостоверяющим центром, является сертификат «Головной удостоверяющий центр». Найти его можно в сети Интернет на Портале уполномоченного федерального органа в области использования электронной подписи по адресу e-trust.gosuslugi.ru/MainCA.

1. Чтобы скачать сертификат, на странице

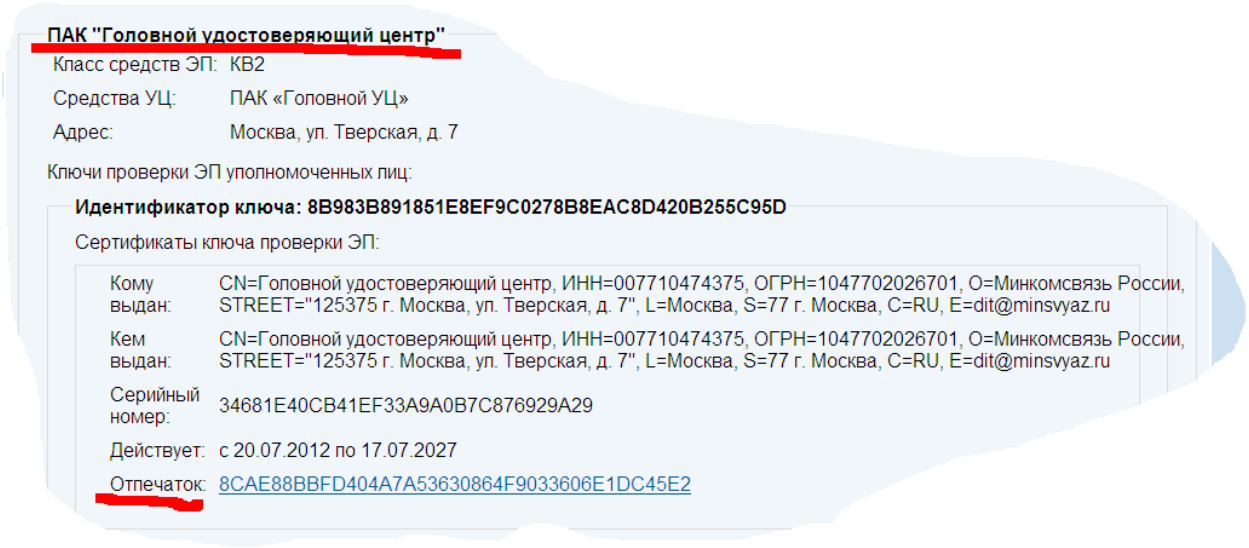


Рисунок 3

необходимо нажать на ссылку «Отпечаток» под заголовком «ПАК «Головной удостоверяющий центр» (см. Рисунок 3). ***Обратите внимание*** на срок действия Сертификата ключа проверки ЭП: в поле «Действует» должен быть актуальный период.

2. В диалоге загрузки файла нажмите кнопку «Открыть» (см. Рисунок 4).

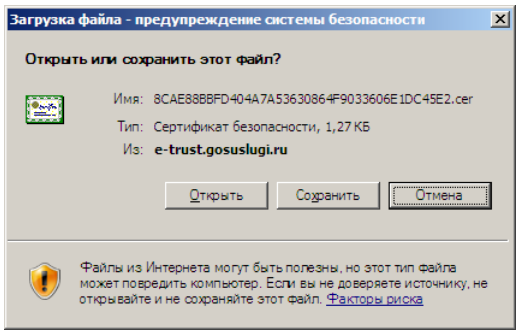


Рисунок 4

3. В открывшемся окне «Сертификат» нажмите кнопку «Установить сертификат» (см. ниже Рисунок 5).

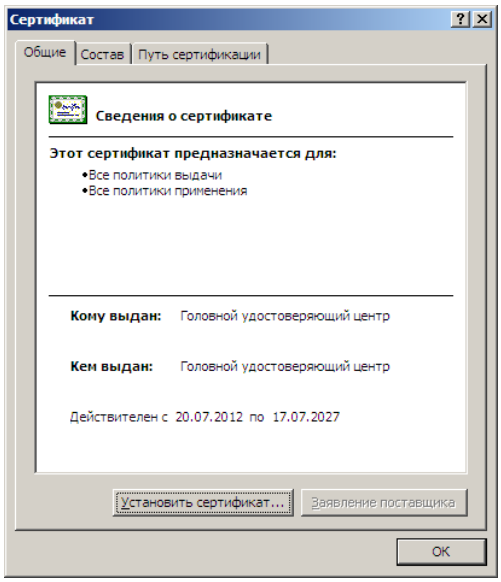


Рисунок 5

4. Далее следуя указаниям «Мастера импорта сертификатов» на первой странице нажмите кнопку «Далее».

5. На странице «Хранилище сертификатов» выберите «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор...» (см. ниже Рисунок 6).

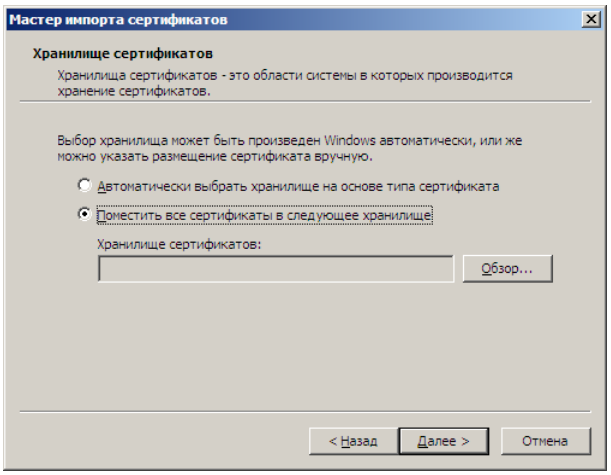


Рисунок 6

6. В окне «Выбор хранилища сертификатов» выберите «Доверенные корневые центры сертификации» и нажмите кнопку «ОК» (см. Рисунок 7). На странице «Хранилище сертификатов» нажмите кнопку «Далее».

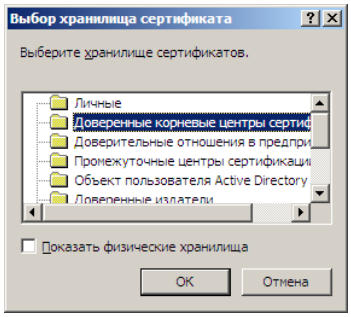


Рисунок 7

7. На странице «Завершение работы мастера импорта сертификатов» нажмите кнопку «Готово» и потом кнопку «ОК».

Корневой сертификат установлен.

6. Установка кросс-сертификата верхнего уровня

На текущий момент Удостоверяющий центр Министерства связи и массовых коммуникаций РФ выпустил два кросс-сертификата верхнего уровня – «УЦ 1 ИС ГУЦ» и «УЦ 2 ИС ГУЦ». В данном примере рассматривается установка «УЦ 1 ИС ГУЦ». Установка кросс-сертификата «УЦ 2 ИС ГУЦ» выполняется аналогично.

Чтобы установить кросс-сертификат, надо выполнить шаги 1 – 6, перечисленные в разделе «Установка корневого сертификата» с некоторыми отличиями.

a. При выполнении шага 1 найти ссылку «Отпечаток» для установки сертификата можно на той же самой странице e-trust.gosuslugi.ru/MainCA под заголовком «ПАК «УЦ 1 ИС ГУЦ». ***Обратите внимание*** на срок действия Сертификата ключа проверки ЭП: в поле «Действует» должен быть актуальный период.
b. При выполнении шага 6 раздела «Установка корневого сертификата» надо выбрать «Промежуточные центры сертификации» (см. Рисунок 8).

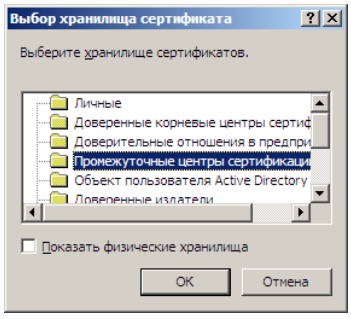


Рисунок 8

Кросс-сертификат верхнего уровня установлен.

7. Установка кросс-сертификата Вашего Удостоверяющего центра

Найти кросс-сертификат Вашего Удостоверяющего центра можно в сети Интернет на Портале уполномоченного федерального органа в области использования электронной подписи по адресу e-trust.gosuslugi.ru/CA, в разделе «Реестры – Аккредитованные УЦ».

Рисунок 9

1. На странице расположен фильтр для поиска нужного Удостоверяющего центра. Введите название Удостоверяющего центра в поле «Псевдоним ПАКа» и нажмите кнопку «Применить» (см. Рисунок 9).

2. Если название введено правильно, на странице появится ссылка на информацию об Удостоверяющем центре.

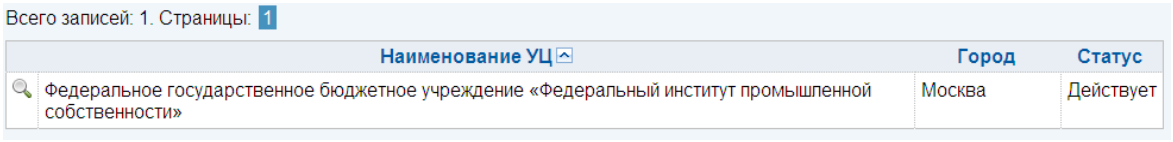


Рисунок 10

Щелкните по изображению увеличительного стекла слева от поля «Наименование УЦ».

3. Найдите на странице информацию о нужном ПАКе и откройте ссылку «Отпечаток» (см. Рисунок 11). ***Обратите внимание*** на срок действия Сертификата ключа проверки ЭП: в поле «Действует» должен быть актуальный период. Если присутствуют несколько сертификатов, выберете самый свежий сертификат.

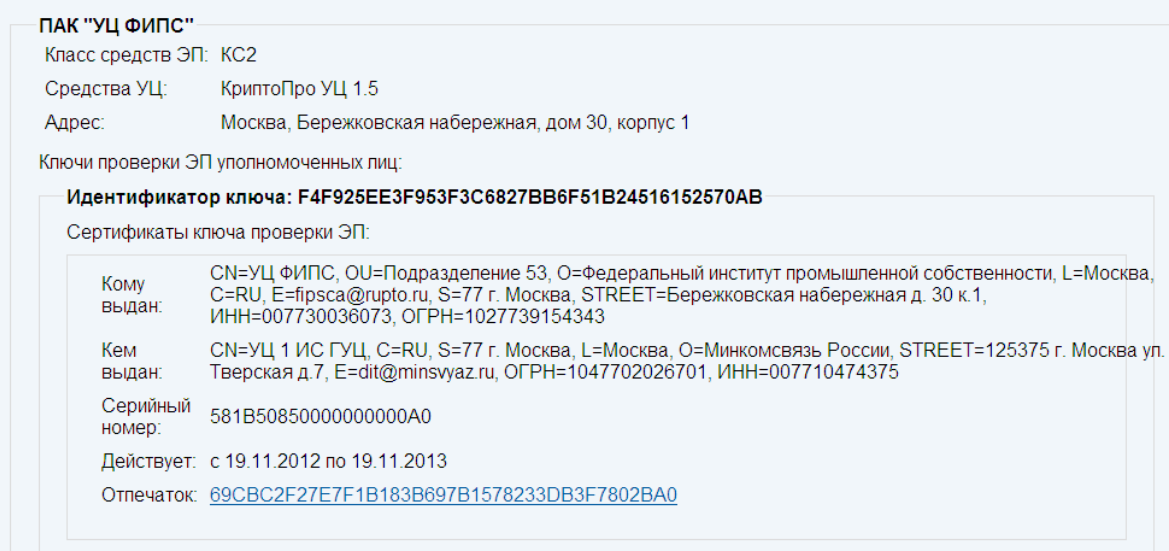


Рисунок 11

4. Далее выполните шаги 2 – 5 из раздела «Установка корневого сертификата».

5. Далее выполните шаг b из раздела «Установка кросс-сертификата верхнего уровня».

6. Далее выполните шаг 7 из раздела «Установка корневого сертификата»

Установка кросс-сертификата Вашего удостоверяющего центра закончена.

7. Установка кросс-сертификата УЦ ФИПС

Для корректной работы КПС РТЗ рекомендуется так же установить кросс-сертификат «УЦ ФИПС», чтобы обеспечить «цепочку доверия» серверному сертификату КПС РТЗ (используется для шифрования канала по протоколу SSL).

Для установки сертификата «УЦ ФИПС» необходимо выполнить все шаги из раздела «Установка кросс-сертификата Вашего Удостоверяющего центра», только в поле «Псевдоним ПАКа» укажите «УЦ ФИПС». Если кросс-сертификат верхнего уровня не был установлен (поле «Кем выдан», часть «CN», см. Рисунок 11), тогда повторите все шаги из раздела «Установка кросс-сертификата верхнего уровня» для соответствующего сертификата.

8. Проверка правильности установки цепочки сертификатов

Чтобы проверить правильность установки сертификатов, откройте консоль управления сертификатами. Например с помощью ярлыка по пути: Пуск → Все программы → Крипт-Про → Сертификаты.

1. Перейдите в хранилище текущего пользователя в папку «Личное» и дважды щелкните левой кнопкой мыши на Вашем Сертификате. В окне «Сертификат» откройте закладку «Путь сертификации».

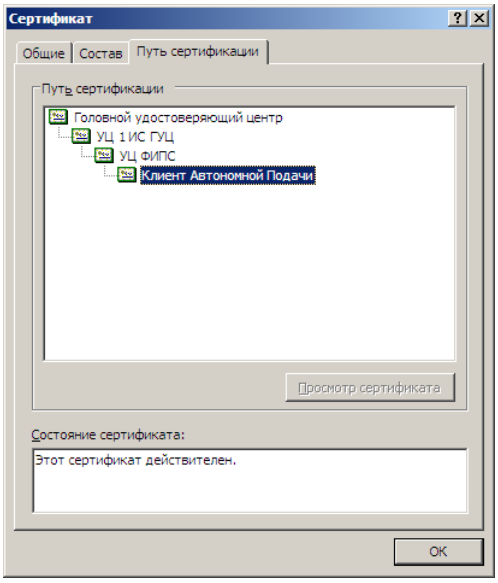


Рисунок 12

Если все сертификаты установлены правильно, закладка «Путь сертификации» должна выглядеть как на Рисунок 12.

Так же убедитесь, что все данные установленного на Вашем компьютере сертификата корректны (правильно указано название УЦ, выдавшего сертификат, ваши персональные данные также должны соответствовать заявленным).

2. Перейдите в папку «Доверенные корневые центры» и убедитесь, что в списке присутствует «Головной удостоверяющий центр» и *отсутствуют* кросс-сертификаты «УЦ 1 ИС ГУЦ», «УЦ 2 ИС ГУЦ» и Вашего удостоверяющего центра.

3. Перейдите в папку «Промежуточные центры сертификации» и убедитесь, что в списке *отсутствует* «Головной удостоверяющий центр» и присутствуют кросс-сертификаты «УЦ 1 ИС ГУЦ» и/или «УЦ 2 ИС ГУЦ» и Вашего удостоверяющего центра.