



КАРМА

Информация по работе с
сертификатами

©Электронные Офисные Системы. 2019 г.

Оглавление

Общая информация	3
Запуск «Консоли управления» и оснастки «Сертификаты».....	3
Выгрузка сертификатов из хранилищ.....	8
Установка сертификата без использования его секретного ключа	12
Установка сертификата средствами системы Windows	12
Автоматическая установка сертификата	12
Установка сертификатов с помощью консоли управления	14
Установка множества сертификатов в хранилище.....	16
Установка сертификата для использования секретного ключа	17
Общая информация	17
Установка сертификатов с закрытым ключом стандартными средствами Windows.....	18
Выгрузка и установка сертификатов с закрытым ключом с использованием средств КриптоПро CSP	20
Работа с корневыми сертификатами.....	25

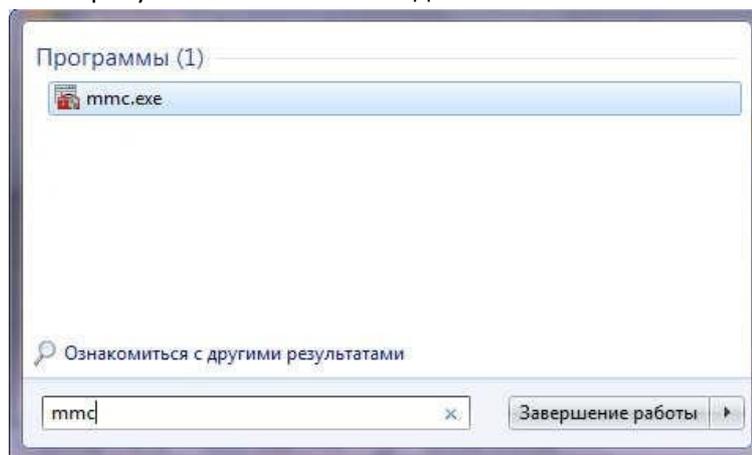
Общая информация

Для корректной работы с цифровыми подписями и зашифрованными контейнерами необходимо, в первую очередь, правильно организовать работу с пользовательскими сертификатами, корневыми сертификатами удостоверяющих центров и списками отзыва. Этот документ поможет в организации работы с сертификатами и их хранилищами, для более подробной информации по работе со списками отзыва следует ознакомиться с документом «Информация по работе со списками отзыва».

Система КАРМА предоставляет пользователю несколько вариантов работы, а также позволяет пользоваться различными хранилищами. В последующих разделах можно узнать, как и куда осуществлять установку сертификатов, что может помочь не только при работе с системой КАРМА, но и с многими другими.

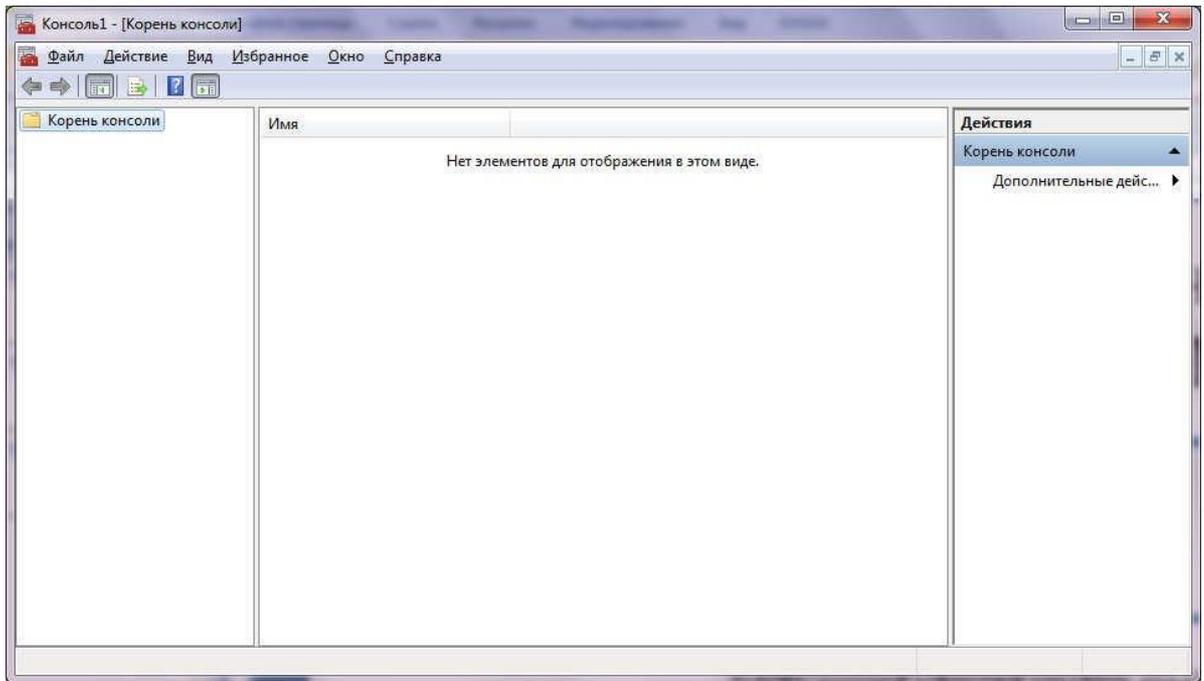
Запуск «Консоли управления» и оснастки «Сертификаты»

В ряде случаев, для удобства работы Вам может потребоваться установить сертификат не в хранилища текущего пользователя, а, например, в хранилища компьютера либо в хранилища системной службы, либо выгрузить сертификат из хранилища, куда он был первоначально установлен, на жесткий диск. Для этого Вам следует использовать «Консоль управления». Для запуска «Консоли управления» в Windows XP и Windows 2003 нажмите «Пуск», затем «Выполнить», введите «mmc» и нажмите «Ок»; Для Windows Vista, Windows 7 и Windows 2008 достаточно нажать «Пуск», ввести «mmc» в строку поиска и нажать Ввод.

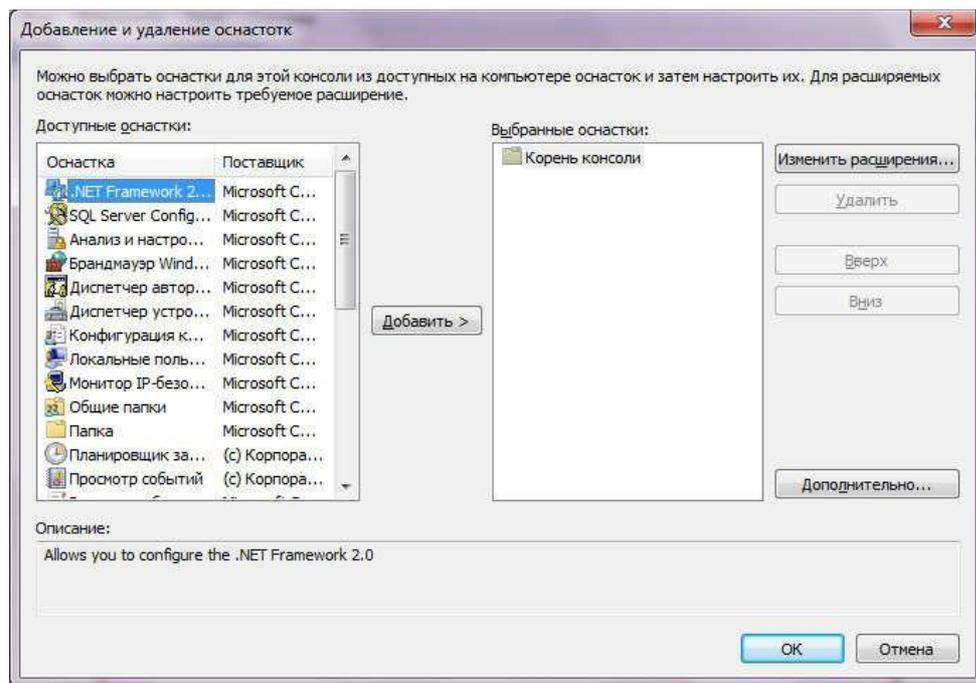


Внимание! Запуск консоли управления и установка сертификата в любые хранилища, отличные от хранилищ текущего пользователя, требует наличия у пользователя прав администратора системы.

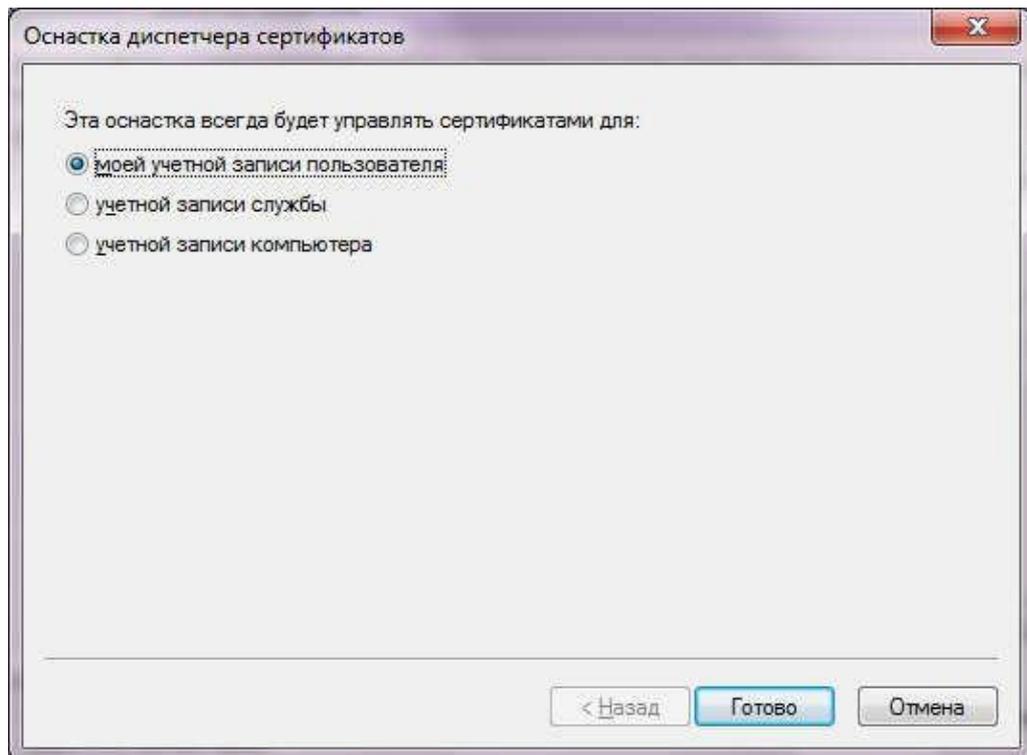
После запуска консоли появится следующее окно:



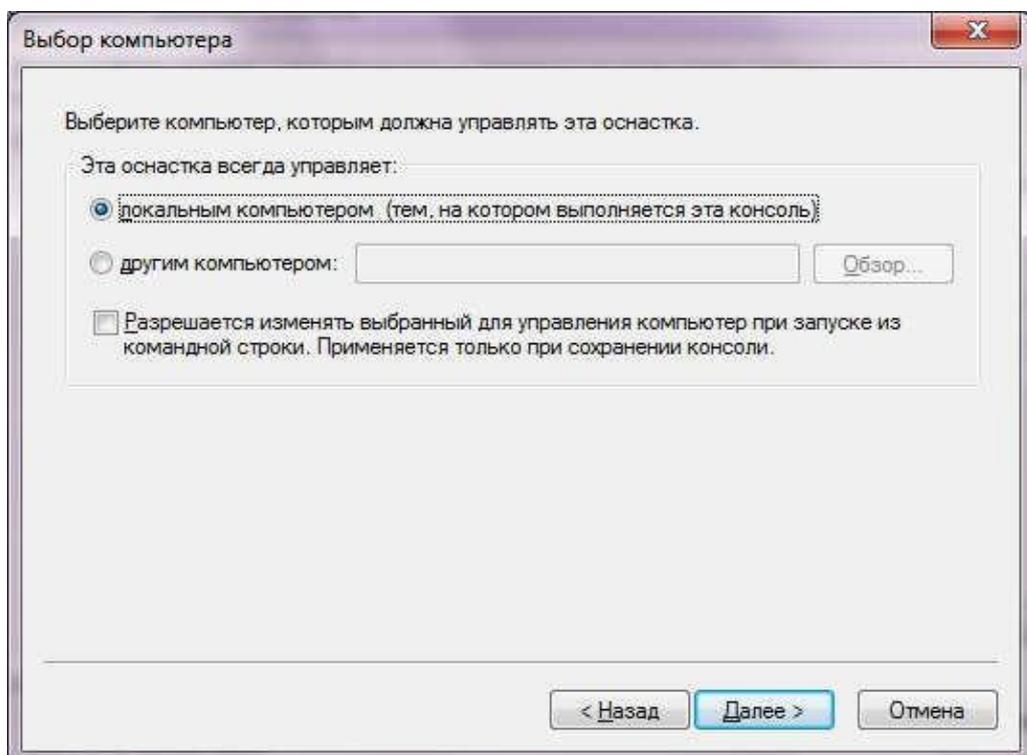
Выберите пункт меню «Файл», далее «Добавить или удалить оснастку» или нажмите сочетание клавиш Ctrl+M. После этого появится следующее окно, содержащее списки оснасток:



Найдите в левом списке оснастку под названием «Сертификаты» и добавьте ее в правый список, нажав кнопку «Добавить»; при этом Вы увидите следующее окно:



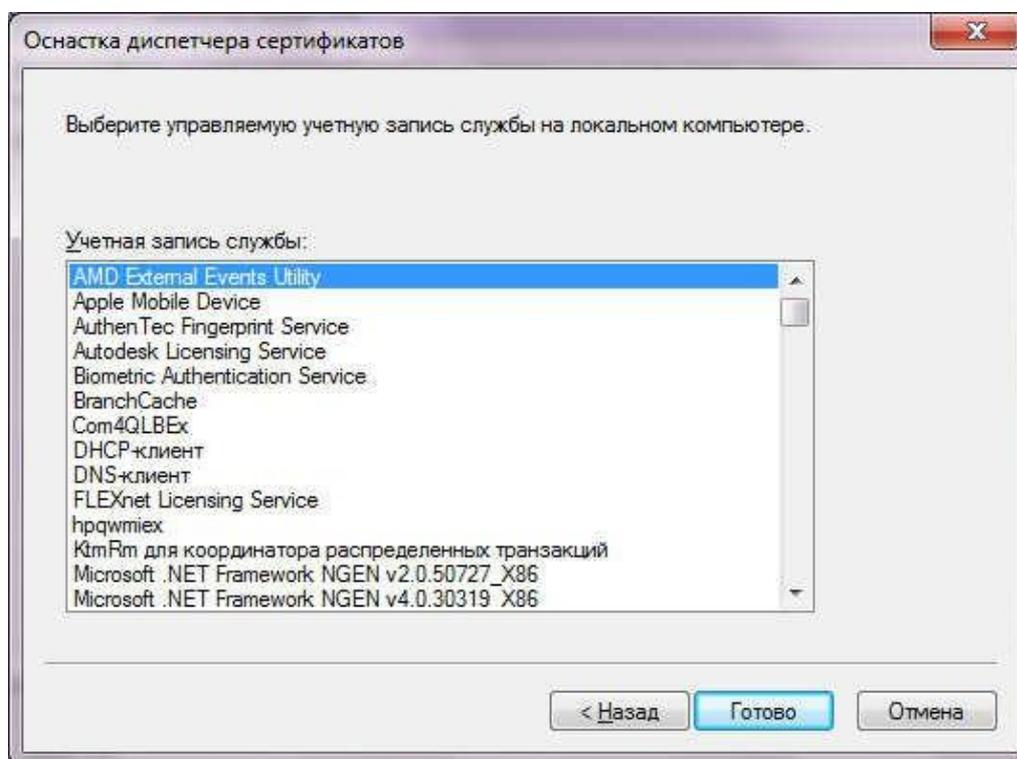
Среди появившихся вариантов выберите интересующий Вас и нажмите «Готово». В случае, если Вы выберете пункт «моей учетной записи пользователя», оснастка будет сразу же добавлена в правый список оснасток. Если же Вы выберете пункты «учетной записи службы» или «учетной записи компьютера», Вы увидите следующее окно:



Выберите подходящий Вам вариант и нажмите «Далее». При этом, в случае выбора варианта «другим компьютером» имя компьютера можно ввести вручную, либо запустить поиск с помощью кнопки «Обзор». На компьютере, к хранилищам которого (либо к хранилищам системной службы

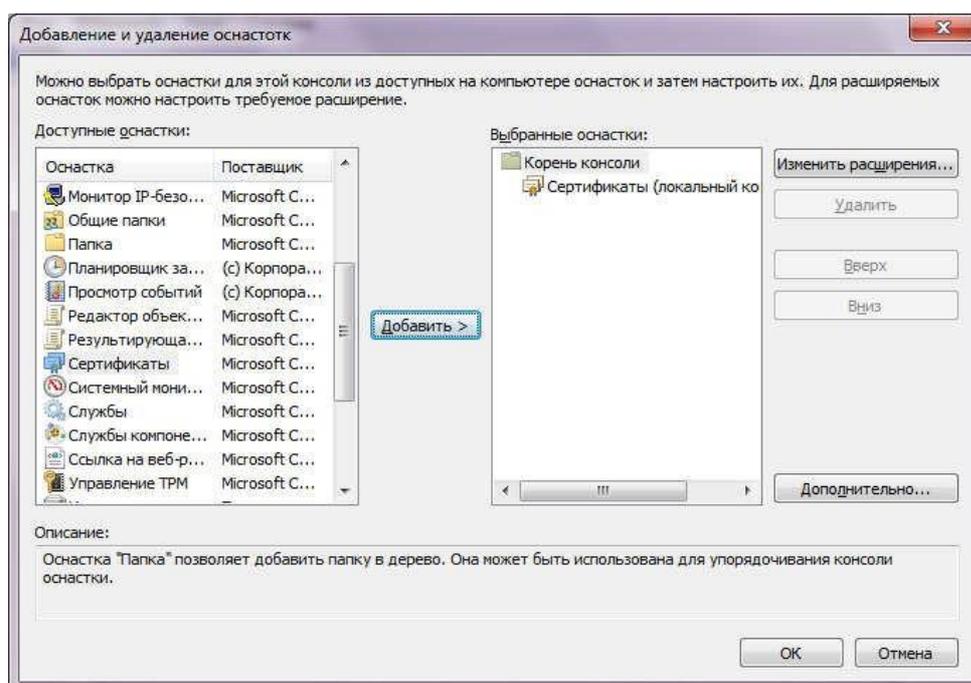
которого) Вы собираетесь обратиться, Вам должен быть дан доступ к соответствующим веткам реестра.

Если Вы на предыдущем экране выбрали вариант «учетной записи службы», то после нажатия кнопки «Далее» Вы увидите следующее окно:



В данном окне представлен список системных служб, доступных на выбранном компьютере. Выберите нужную Вам системную службу и нажмите «Готово».

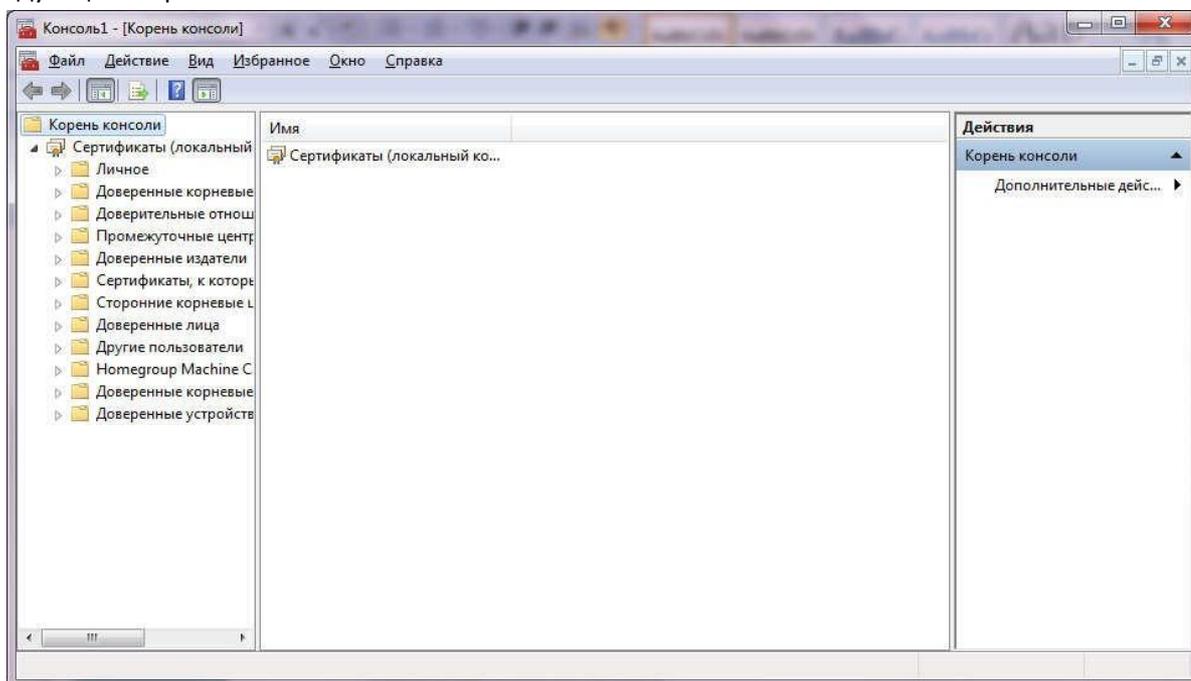
Теперь в правом списке появилась только что настроенная оснастка:



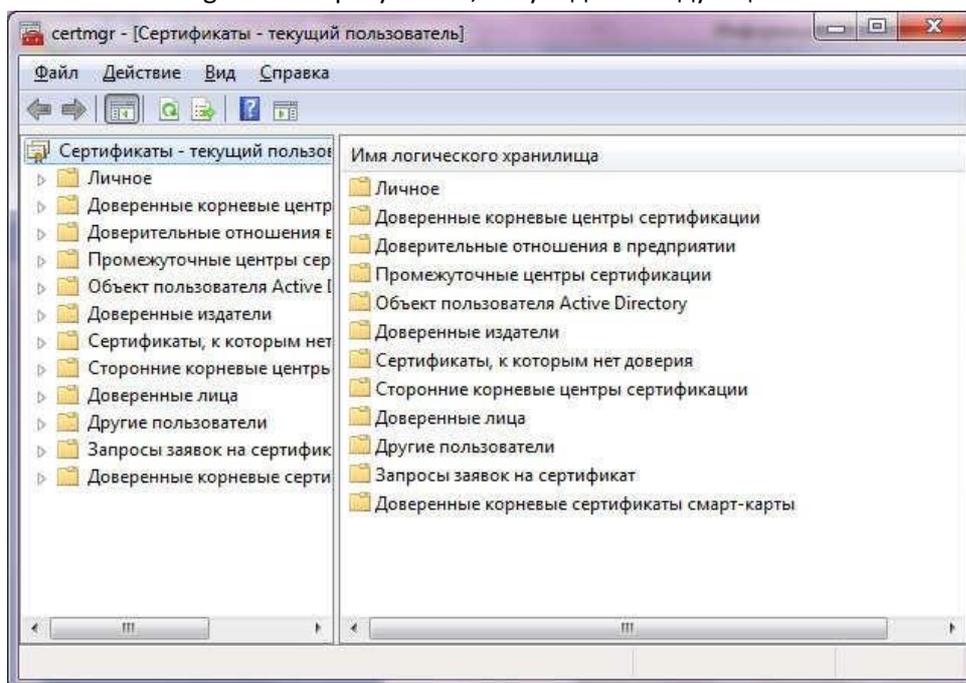
Вы можете добавить оснастку «Сертификаты» несколько раз для работы с сертификатами в хранилищах, расположенные в отличном от первого месте. К примеру, Вы можете одновременно

брать сертификаты из хранилища текущего пользователя и загружать их в хранилища системной службы на удаленном компьютере.

После того, как Вы добавите нужное Вам количество оснасток, нажмите «Ок». Консоль будет подготовлена к работе с хранилищами сертификатов, а основное окно консоли будет выглядеть следующим образом:



Внимание! Для управления сертификатами текущего пользователя можно воспользоваться непосредственным запуском соответствующей оснастки. Для этого, вместо «mmc» наберите в строке выполнения «certmgr.msc». В результате, Вы увидите следующее окно:



В данном окне возможны все те же операции, что и при добавлении соответствующей оснастки «Сертификаты» в «Консоль управления».

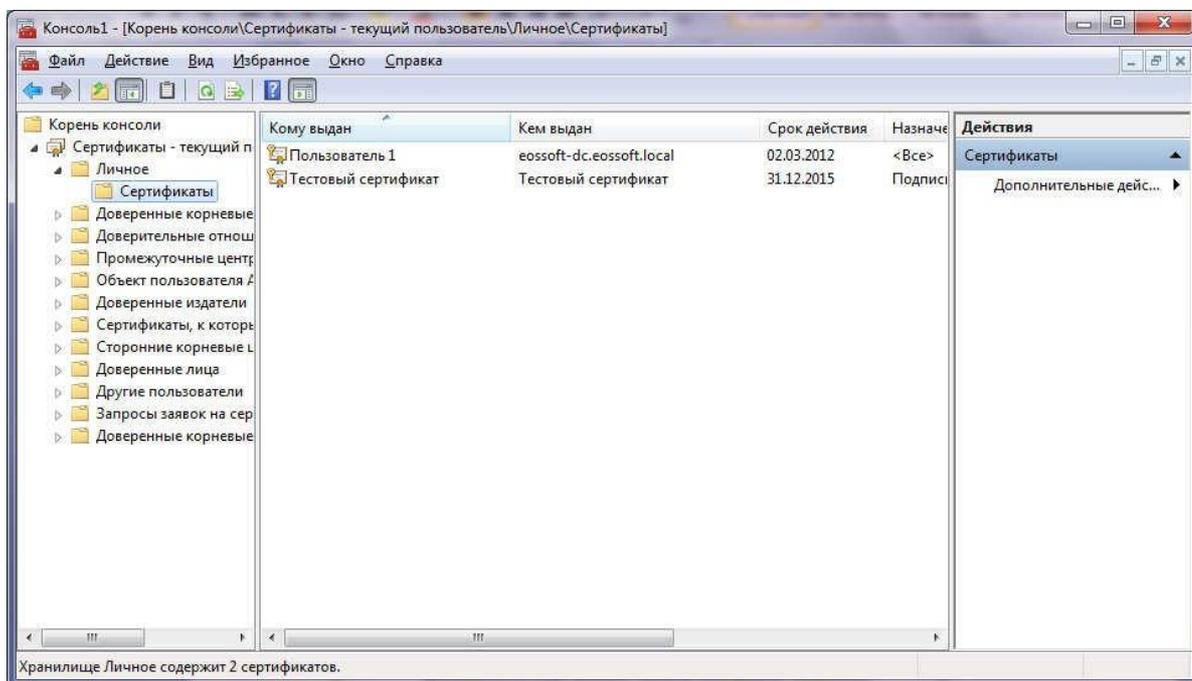
Выгрузка сертификатов из хранилищ

Выгрузка сертификатов на диск – достаточно часто проводимая операция, целью которой в большинстве случаев является получение файла собственного сертификата для дальнейшей отправки получателю подписанных вами писем, или отправляющему Вам зашифрованные сообщения адресату. В этом случае выгружать сертификаты требуется без экспорта секретного ключа. Однако, в ряде случаев, возникает необходимость получить сертификат и его секретный ключ с удостоверяющего центра на одном компьютере, а использовать на другом, например при централизованном получении сертификатов. В таком случае встает задача выгрузки сертификата с секретным ключом.

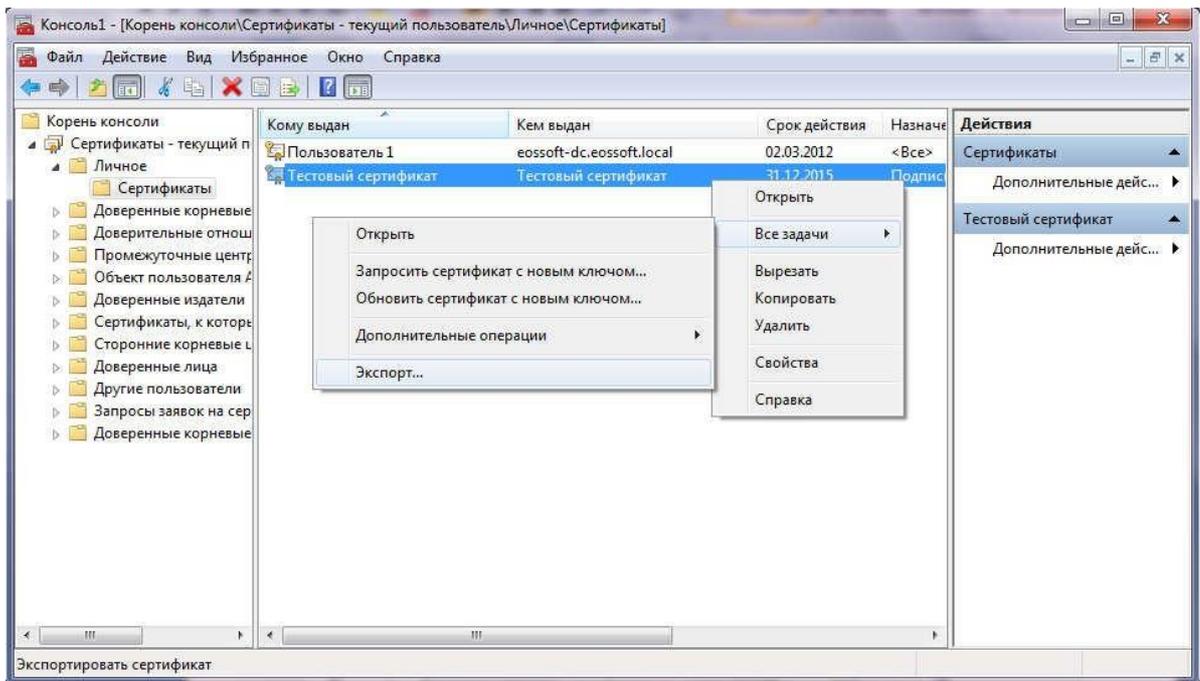
Логика работы с сертификатами системы Windows предполагает, по-умолчанию, использование сертификата с закрытым ключом на том компьютере, на котором он был получен. Однако, если при получении сертификата закрытый ключ этого сертификата был помечен как экспортируемый, система позволяет выгрузить сертификат и закрытый ключ в один файл с расширением «.pfx», и, в дальнейшем, установить его на другой компьютер.

Внимание! Обратите внимание, что некоторые криптопровайдеры, например, КриптоПро CSP, блокируют работу с экспортируемыми закрытыми ключами.

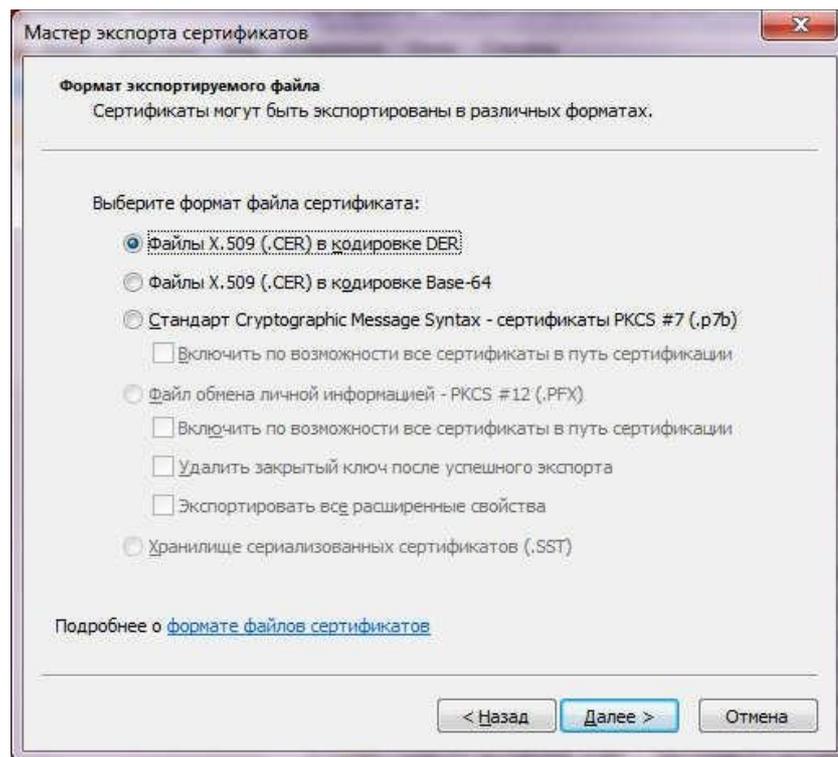
Рассмотрим операцию экспорта сертификата и сохранения его на диск на примере экспорта из личного хранилища пользователя. Откройте консоль управления и добавьте в нее оснастку «Сертификаты» для управления хранилищами «моей учетной записи пользователя» (подробнее о запуске консоли управления в разделе «Запуск «Консоли управления» и оснастки «Сертификаты»). Далее, откройте подпапку «Сертификаты» в папке «Личное»:



Щелкните правой кнопкой мыши на сертификат, который хотите экспортировать, и в появившемся меню выберите пункт «Все задачи», затем «Экспорт»:



В появившемся мастере нажмите кнопку «Далее», после чего Вы увидите следующую страницу мастера экспорта:



При экспорте сертификата возможен выбор нескольких форматов сохранения сертификата.

При выборе пункта «Файлы X.509 (.CER) в кодировке DER» сертификат будет сохранен в наиболее простом формате, без каких либо кодировок, кроме системной. Итоговый файл будет содержать только сам экспортируемый сертификат.

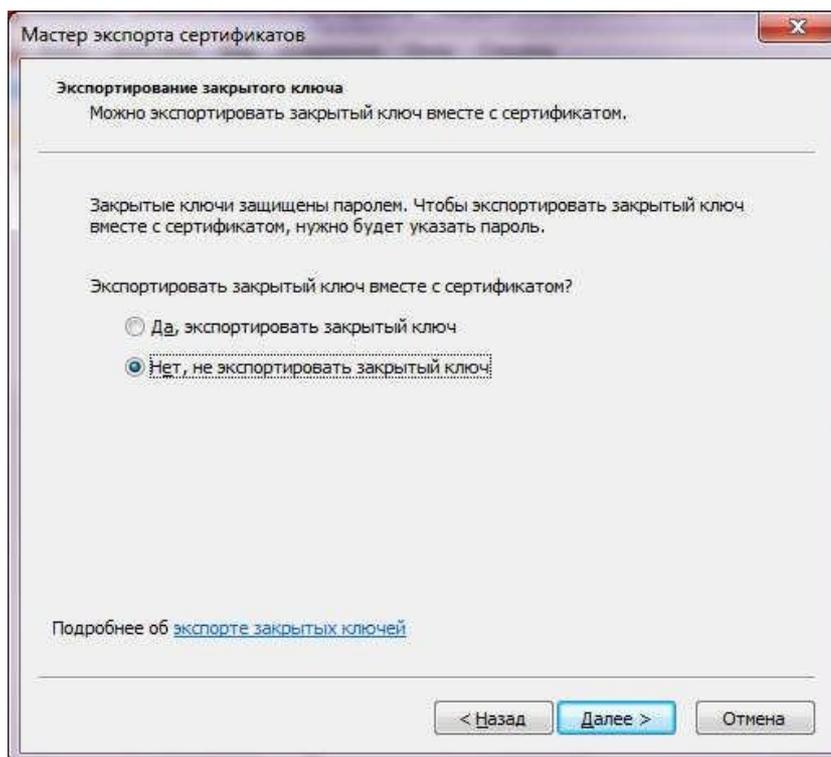
При выборе пункта «Файлы X.509 (.CER) в кодировке Base-64» экспорт происходит аналогично первому случаю, однако сертификат дополнительно кодируется в кодировку Base-64, что может

облегчить хранение данного файла сертификата в базах данных, так как сертификат будет закодирован в текстовую строку.

Пункт «Стандарт Cryptographic Message Syntax – сертификаты PKCS #7 (.p7b)» позволяет экспортировать в один файл несколько сертификатов из хранилища, для их дальнейшего переноса. Таким образом, можно облегчить перенос большого количества сертификатов с одной машины на другую. Кроме того, если взведена галочка «Включить по возможности все сертификаты в путь сертификации», система Windows помимо непосредственно выбранных сертификатов сохранит в файл всю доступную на данной машине цепочку сертификатов, от корневого до пользовательского, включая промежуточные, что еще более облегчит использование данных сертификатов на машине, куда они будут перенесены.

Выбор пункта «Файл обмена личной информацией – PKCS #12 (.PFX)» доступен только в случае, если при получении сертификата с удостоверяющего центра, либо при установке его в хранилище закрытый ключ, связанный с сертификатом, был помечен как экспортируемый, либо выбрано несколько сертификатов.

Внимание! Если сертификат связан с закрытым ключом, а ключ помечен как экспортируемый, то при экспорте сертификата вторая страница будет выглядеть следующим образом:



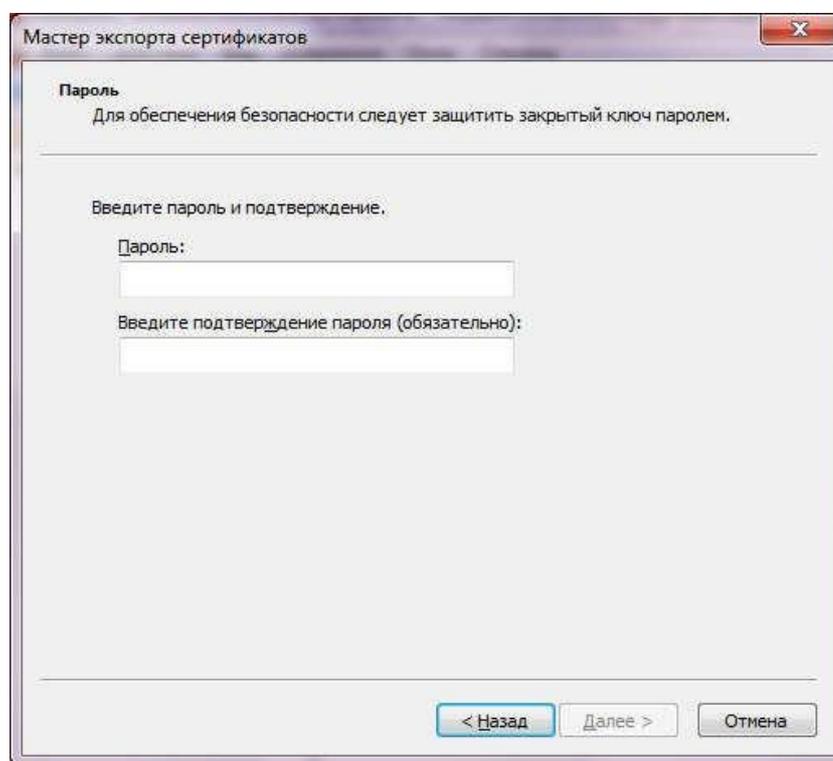
Для того, чтобы на следующей странице стал доступен пункт «Файл обмена личной информацией – PKCS #12 (.PFX)», на данной странице необходимо выбрать пункт «Да, экспортировать закрытый ключ». В противном случае, пункт будет недоступен, а страница мастера будет выглядеть так же, как бы она выглядела для сертификата без привязанного секретного ключа.

В данном случае итоговый файл, помимо самого сертификата, будет содержать также и закрытый ключ, связанный с ним, и данный контейнер может быть использован для переноса сертификата на компьютер, на котором планируется его использование для операций подписания, шифрования

или расшифровывания. Если взведена галочка «Удалить закрытый ключ после успешного экспорта», то после экспорта закрытый ключ на данном компьютере будет удален, и использование сертификата для подписания, шифрования или расшифровывания на данной машине станет невозможным. Галочка «Экспортировать все расширенные свойства» предоставляет возможность выбрать, экспортировать ли сертификат со всеми его расширениями, либо без них. Данная настройка предназначена для опытных пользователей, не рекомендуется изменять ее самостоятельно.

Пункт «Хранилище сериализованных сертификатов (.SST)» доступен только при выборе одновременно нескольких сертификатов для экспорта. В данном случае формируется временное хранилище сертификатов, в котором они представлены в сериализованном виде, что может быть удобно для работы с данными сертификатами из различных приложений.

Выберите необходимый пункт меню и нажмите «Далее». В случае, если Вы экспортируете сертификат с закрытым ключом, Вы увидите следующую страницу мастера (если Вы не экспортируете закрытый ключ вместе с сертификатом, данная страница будет пропущена):



Мастер экспорта сертификатов

Пароль
Для обеспечения безопасности следует защитить закрытый ключ паролем.

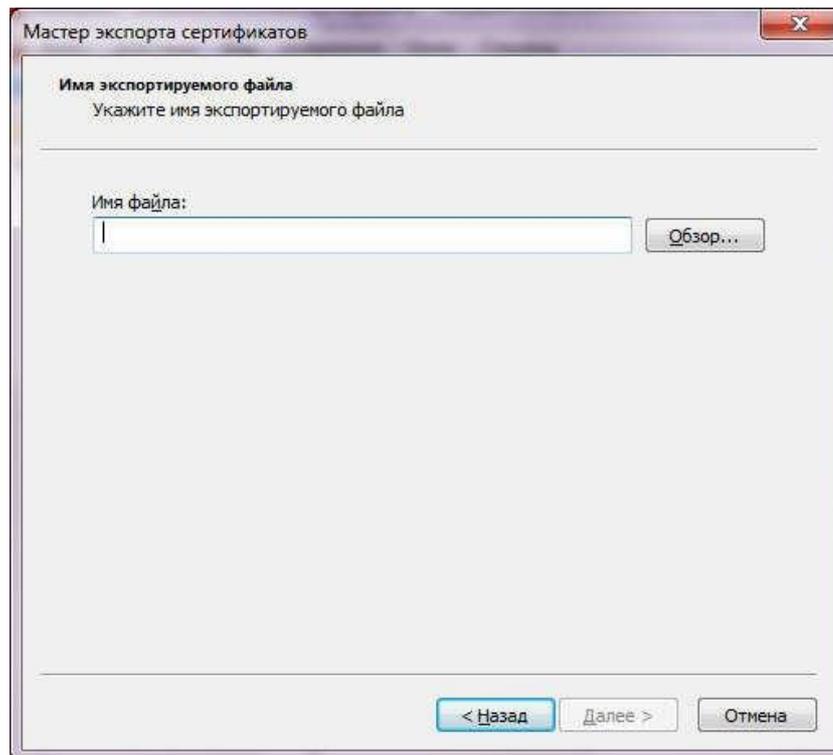
Введите пароль и подтверждение.

Пароль:

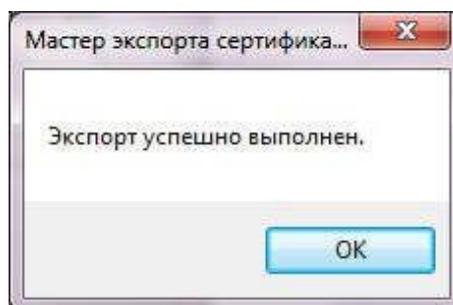
Введите подтверждение пароля (обязательно):

< Назад Далее > Отмена

Если пароль на данной странице не введен, мастер не позволяет продолжить выполнение. Введите пароль и нажмите кнопку «Далее».



На данной странице нажмите кнопку «Обзор» и выберите место и имя файла, в который следует сохранить экспортируемые сертификаты, и нажмите «Далее». Вы увидите страницу с отчетом о проведенной операции экспорта. Нажмите «Готово». Вы увидите сообщение об успешном экспорте сертификатов:

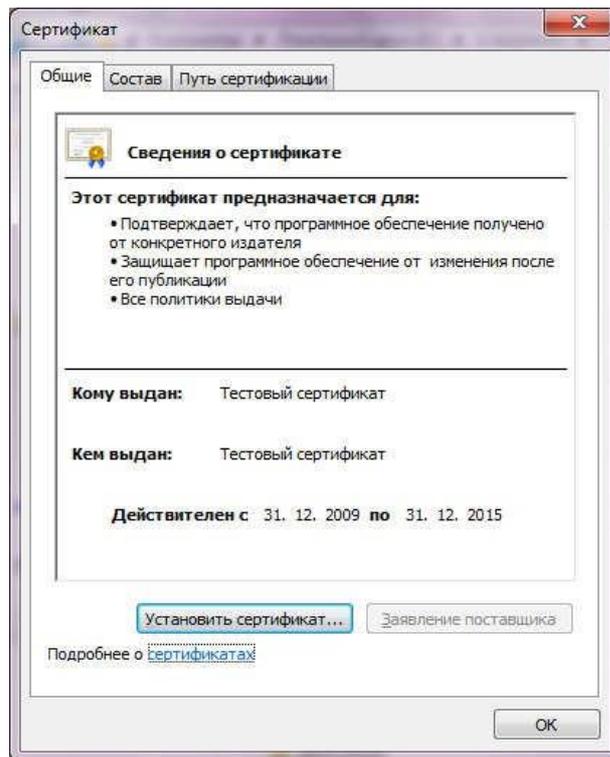


Установка сертификата без использования его секретного ключа

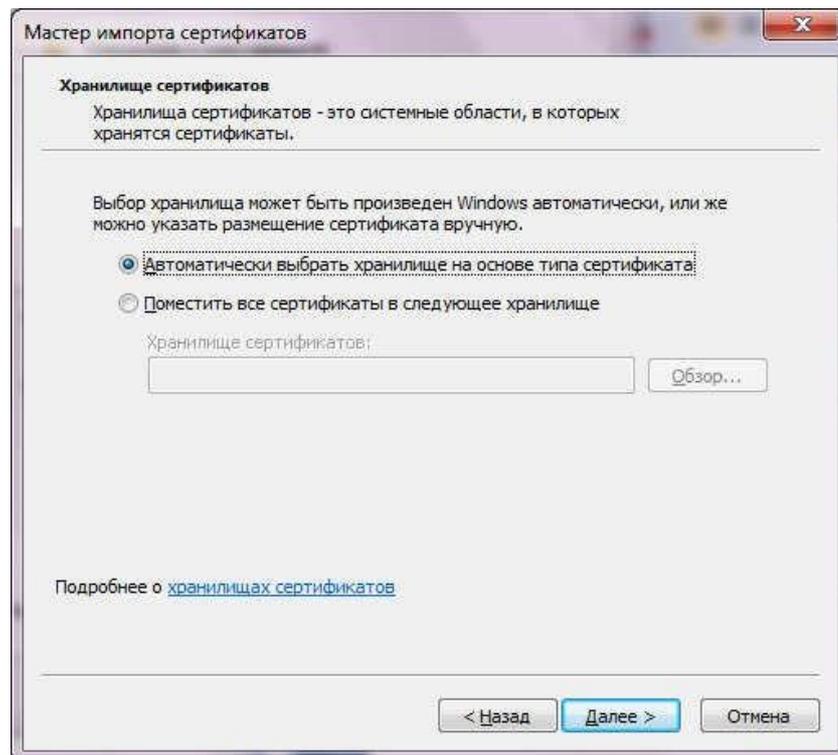
Установка сертификата средствами системы Windows

Автоматическая установка сертификата

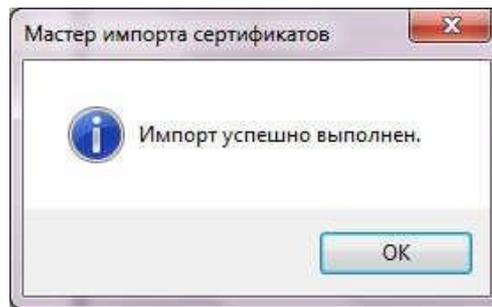
Подобным образом устанавливать сертификаты может потребоваться для проверки полученной Вами цифровой подписи. Для установки сертификата в личное хранилище пользователя дважды щелкните по файлу сертификата. Вы увидите следующий системный диалог:



Нажмите кнопку «Установить сертификат» и в появившемся окне нажмите «Далее». Вы попадете на вторую страницу мастера установки сертификатов:



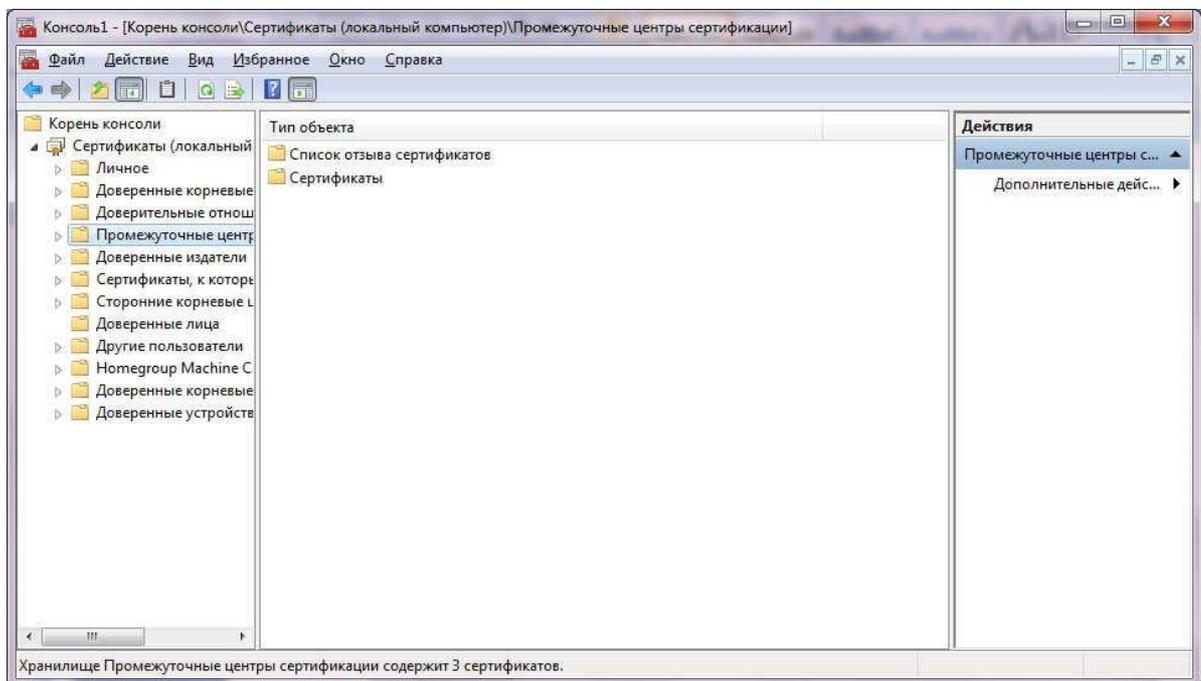
Для установки пользовательского сертификата в личное хранилище пользователя не изменяйте выбранный пункт «Автоматически выбрать хранилища на основе типа сертификата» и нажмите кнопку «Далее» и, на следующей странице, кнопку «Готово». В случае успешной установки Вы увидите следующее сообщение:



Установленный сертификат появится в списке сертификатов хранилища, в которое он был установлен. Для просмотра сертификатов, находящихся в хранилищах следует воспользоваться «Консолью управления» и оснасткой «Сертификаты».

Установка сертификатов с помощью консоли управления

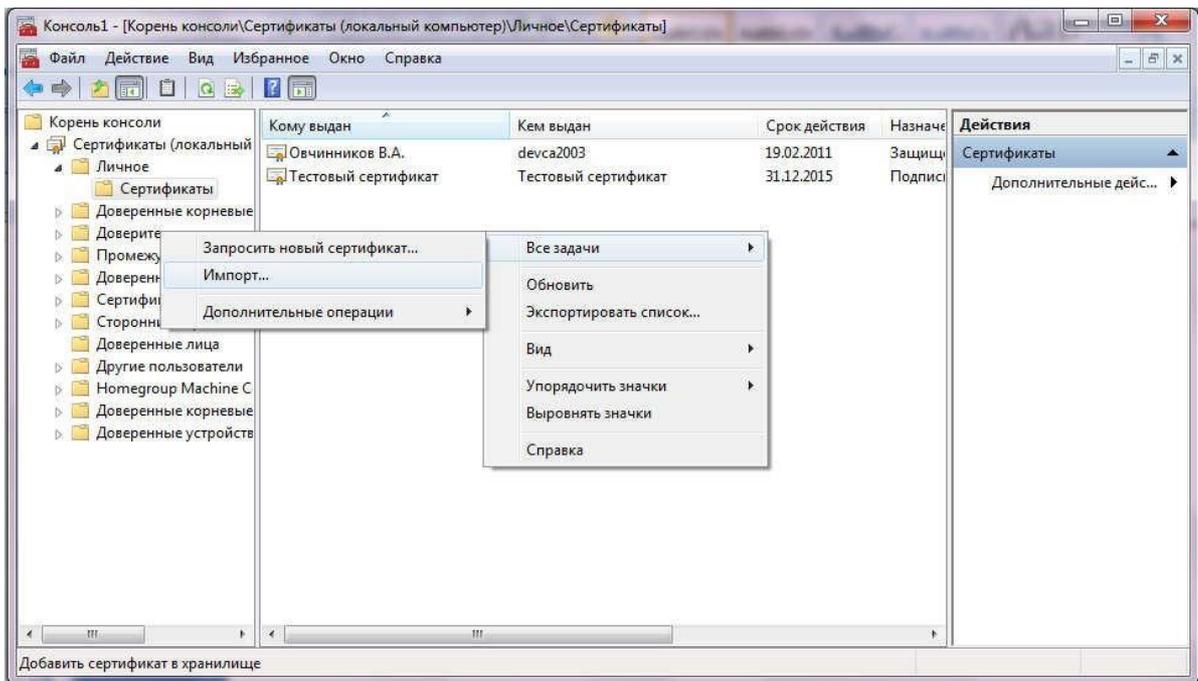
Выберите нужное Вам хранилище в дереве хранилищ в оснастке «Сертификаты». В случае, если в выбранном хранилище уже присутствуют какие-либо объекты, Вы увидите в окне «Тип объекта» папки с соответствующими названиями:



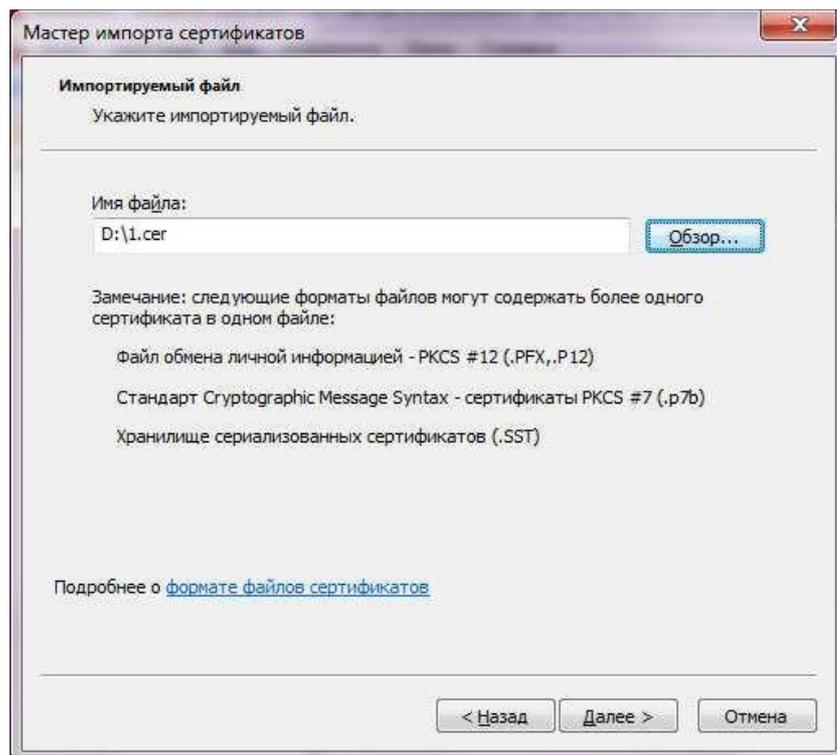
Для добавления сертификатов в хранилище необходимо открыть подпапку «Сертификаты».

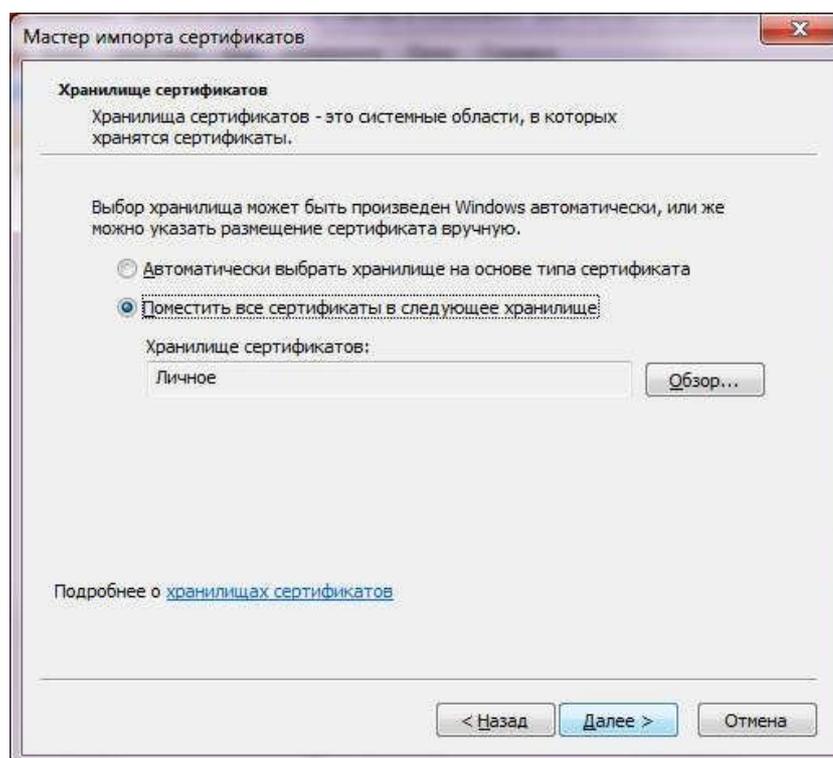
Если сертификаты в хранилище отсутствуют, Вы увидите надпись «Нет элементов для отображения в этом виде». В таком случае, Вы может добавлять сертификаты в хранилище без открытия папки. Папка будет создана автоматически.

Для добавления сертификата в хранилище нажмите правой кнопкой в среднем поле окна и выберите в появившемся меню пункт «Все задачи», подпункт «Импорт...»:

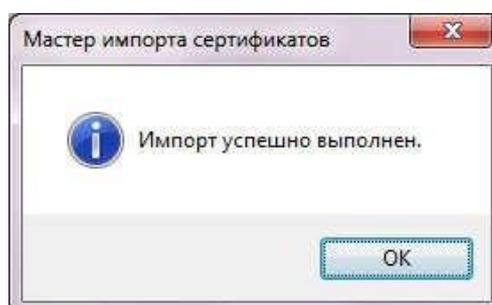


В появившемся окне нажмите «Далее», выберите файл сертификата, который Вы хотите импортировать и вновь нажмите «Далее»:





Не изменяйте выбранный пункт на данной странице настроек, если не хотите действительно изменить хранилище, в которое Вы хотите загрузить сертификат. Нажмите кнопку «Далее», и, на следующей странице, нажмите кнопку «Готово». Вы увидите сообщение об успешном завершении операции:



В списке сертификатов Вы увидите добавленный только что сертификат.

Помимо импорта сертификатов, Вы можете переносить и копировать сертификаты из одного хранилища в другое так же, как это происходит с файлами в проводнике, а также удалять сертификаты.

Установка множества сертификатов в хранилище

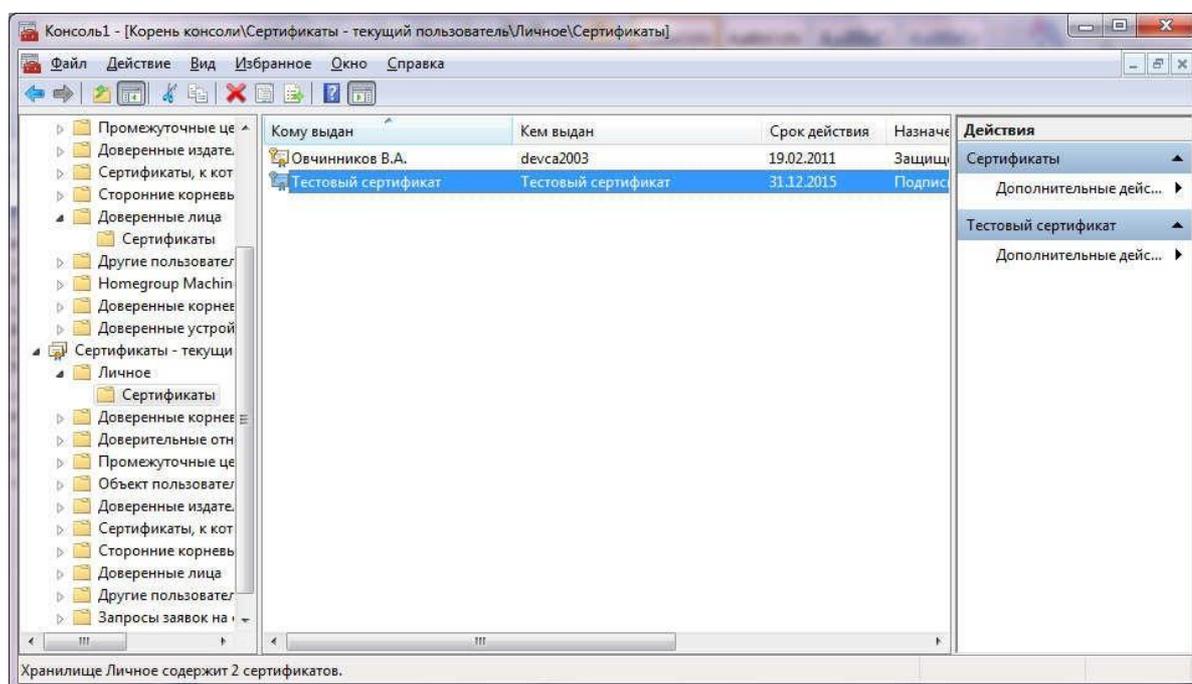
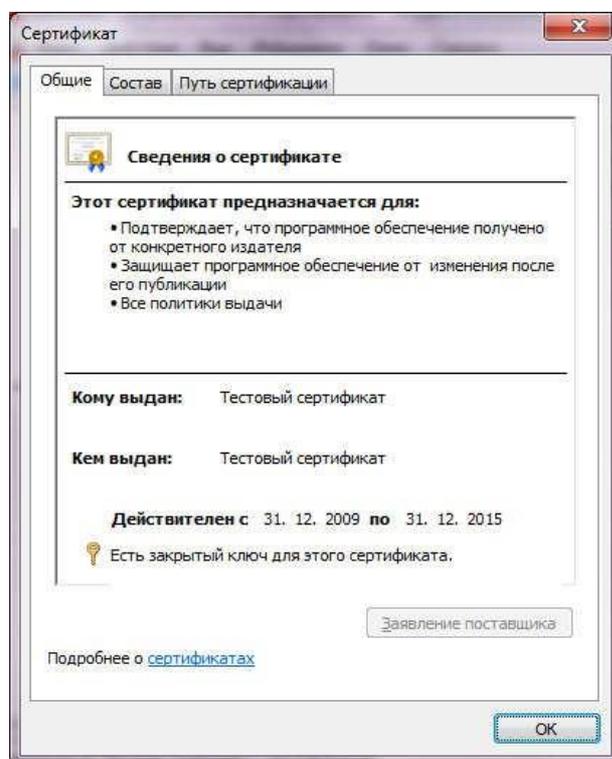
Оснастка Windows не позволяет загрузить сразу множество сертификатов (множество файлов сертификатов) в хранилище. Поэтому, если у Вас возникла такая необходимость, воспользуйтесь утилитой «Утилита импорта сертификатов», которую можно бесплатно скачать с сайта ЭОС <http://www.eos.ru>.

Если же Вам необходимо перенести с одного компьютера на другой несколько сертификатов из хранилища в хранилище, экспортируйте их в формате PKCS #7 (.p7b), который позволяет сохранять несколько сертификатов из хранилища в один файл.

Установка сертификата для использования секретного ключа

Общая информация

Секретный ключ, связанный с сертификатом понадобится Вам для осуществления операций подписания, шифрования и расшифровывания. При просмотре сертификата, для которого привязан секретный ключ, можно увидеть значок ключа и надпись «Есть закрытый ключ для этого сертификата», а в оснастке «Сертификаты» изменяется значок на значок с ключом:



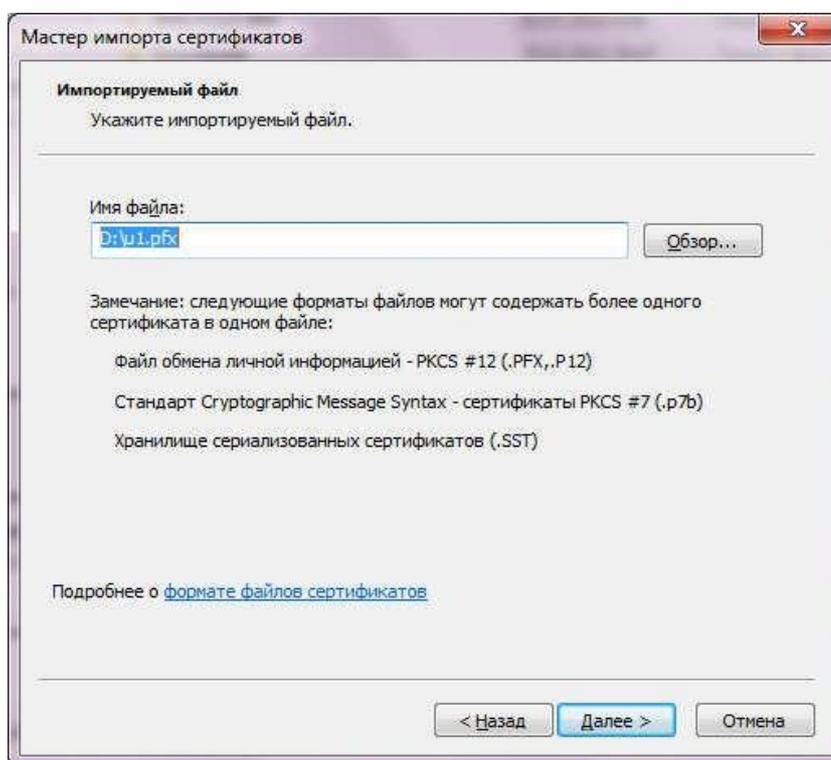
При получении сертификата на удостоверяющем центре, закрытый ключ создается непосредственно на компьютере, с которого отправляется запрос на удостоверяющий центр. Таким образом, полученные с удостоверяющего центра сертификаты уже привязаны к закрытым ключам.

Однако, достаточно часто может потребоваться перенос сертификатов с одного компьютера на другой. В данном документе Вы сможете ознакомиться с выгрузкой и загрузкой сертификата с созданием связи с секретным ключом стандартными способами (средства системы Windows), а также с использованием оснастки криптопровайдера КриптоПро CSP. Для работы с другими криптопровайдерами следует ознакомиться с их пользовательской документацией.

Внимание! Внимательно ознакомьтесь с данным разделом, так как обычного экспорта сертификата и установки его на другую машину недостаточно для дальнейшей работы с ним, т.е. попытка операций подписания, шифрования и расшифровывания с помощью таких сертификатов будет приводить к ошибке.

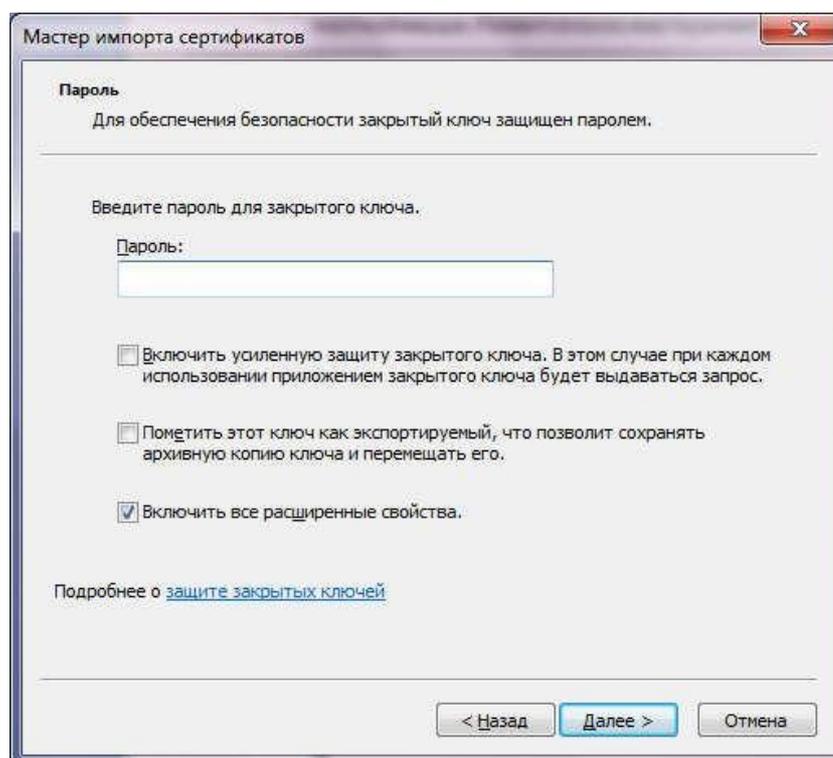
Установка сертификатов с закрытым ключом стандартными средствами Windows

Для начала установки сертификата на компьютер дважды щелкните по файлу «.pfx» левой кнопкой мыши. Появится окно мастера импорта сертификата. На первой странице мастера нажмите «Далее».



На данной странице мастера предоставляется возможность выбрать файл сертификата. Так как мастер был запущен непосредственно из файла сертификата и закрытого ключа, имя файла уже прописано. Однако, Вы можете запустить мастер импорта из оснастки «Сертификаты», и, в таком случае, будет необходимо указать путь к файлу сертификата с закрытым ключом.

Выберите и проверьте имя файла и нажмите «Далее». Вы увидите следующую страницу:



Если при экспорте сертификата с закрытым ключом на полученный контейнер был установлен пароль, то для импорта необходимо ввести данный пароль. Если же пароль установлен не был, это поле нужно оставить пустым.

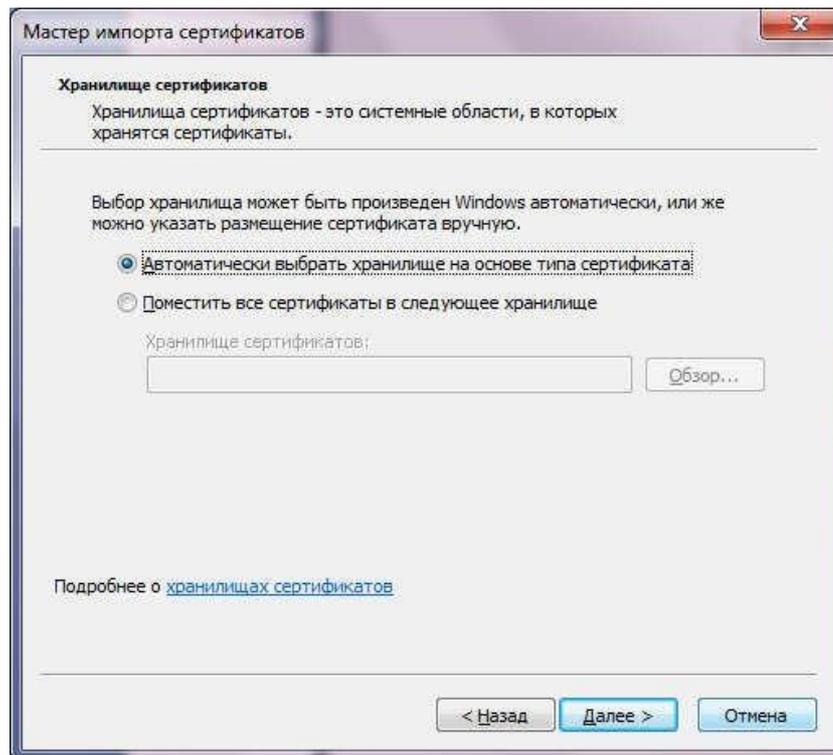
Внимание! Старайтесь всегда при экспорте сертификата с закрытым ключом устанавливать пароли на полученный контейнер. Если этот контейнер по каким-либо причинам попадет в руки злоумышленника, он получит возможность беспрепятственно пользоваться вашим сертификатом.

При установке галочки «Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании приложением закрытого ключа будет выдаваться запрос система попросит Вас ввести отдельный пароль на использование закрытого ключа. Не зная этого пароля, подписать что-либо вашей подписью невозможно. Установка данной галочки возможна, если при получении сертификата на удостоверяющем центре была включена усиленная защита закрытой части ключа.

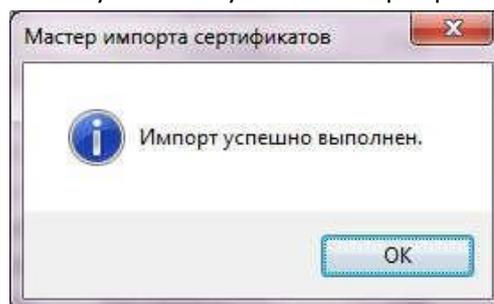
При установке галочки «Пометить этот ключ как экспортируемый, что позволит сохранять архивную копию ключа и перемещать его» появляется возможность экспортировать сертификат с закрытой частью ключа из хранилища сертификатов. Это может потребоваться в случае, если Вы планируете дальнейший перенос сертификата с секретным ключом на другой компьютер, однако по каким-либо причинам не можете для этого воспользоваться уже существующим контейнером «.pfx».

Галочка «Включить все расширенные свойства» предоставляет возможность выбрать, устанавливать ли сертификат со всеми его расширениями, либо без них. Данная настройка предназначена для опытных пользователей, не рекомендуется изменять ее самостоятельно.

После выбора настроек импорта сертификата, нажмите «Далее». Вы увидите страницу выбора хранилища сертификатов, в которое следует установить данный сертификат.



Выберите хранилище и нажмите кнопку «Далее» и, на следующей странице мастера, кнопку «Готово». Вы увидите сообщение об успешной установке сертификата:

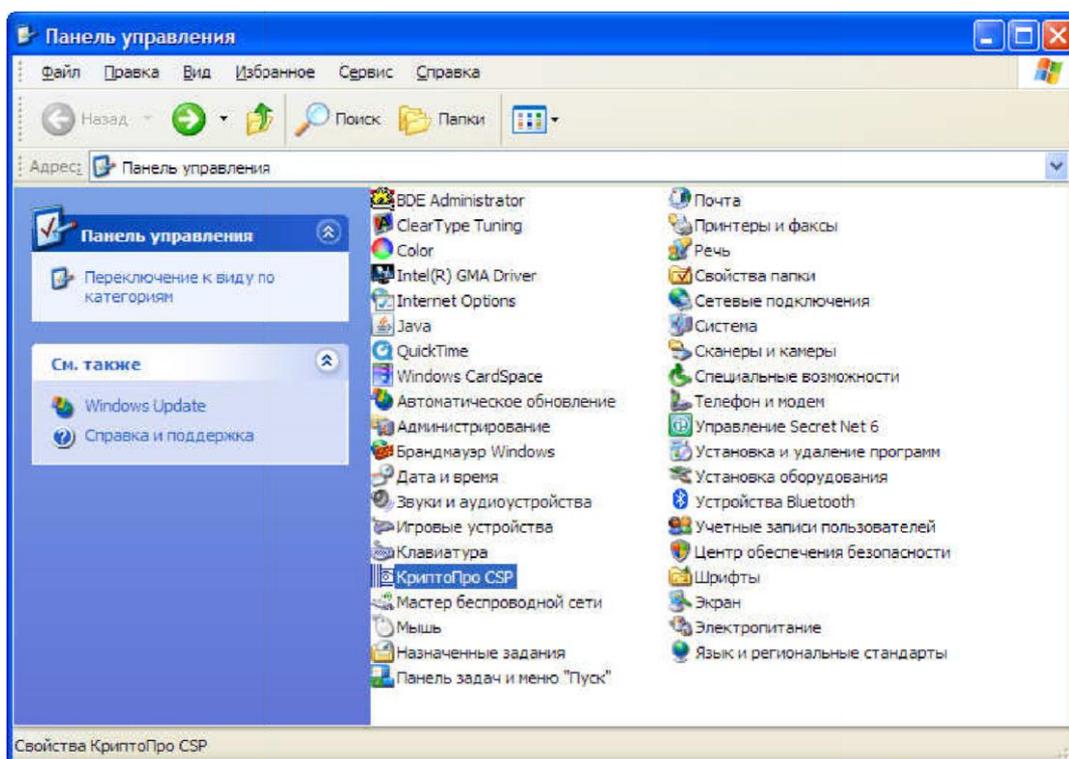


Внимание! В контейнере с расширением «.rfx» помимо самого сертификата может находиться корневой сертификат удостоверяющего центра, выдавшего соответствующий пользовательский сертификат. При установке пользовательского сертификата из данного контейнера, будет произведена попытка автоматической установки корневого сертификата, и будут показаны соответствующие предупреждения. Для более подробной информации по установке корневого сертификата, а также предупреждениям, возникающим в процессе установки, обратитесь к пункту «Установка корневых сертификатов».

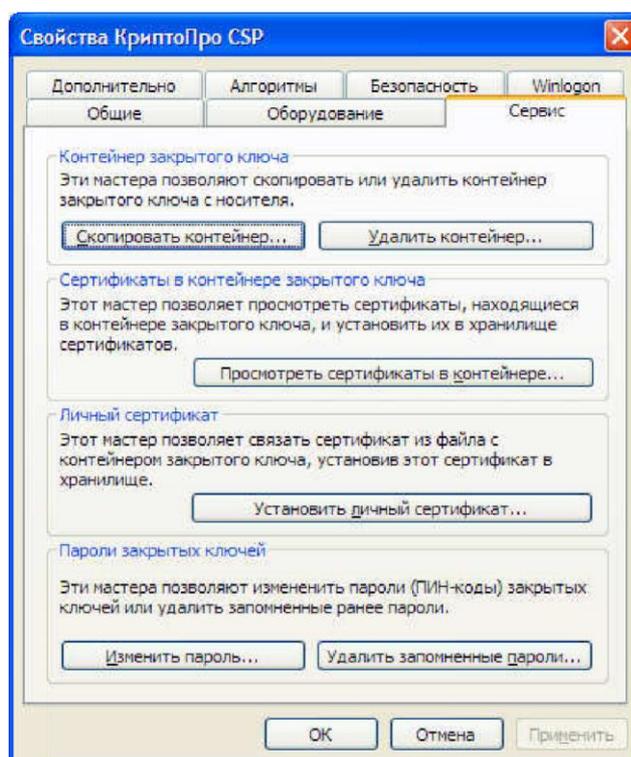
Выгрузка и установка сертификатов с закрытым ключом с использованием средств КриптоПро CSP

В данном варианте не накладывается никаких ограничений на процесс выгрузки сертификата, так как КриптоПро CSP не поддерживает работу с экспортируемыми ключами и работает по собственной схеме.

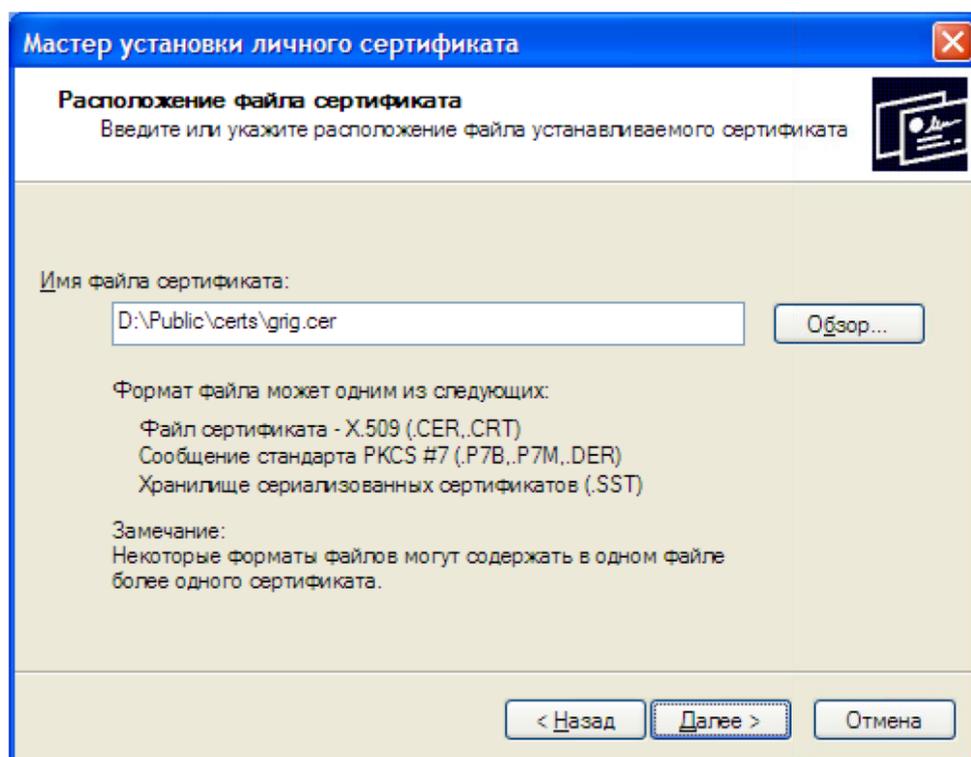
Выгрузите сертификат в файл, выбрав в процессе опцию «Нет, не экспортировать закрытый ключ». В случае, если закрытый ключ при получении сертификата был помечен как экспортируемый, и будет выбран пункт «Да, экспортировать закрытый ключ», этот параметр будет проигнорирован. Полученный файл перенесите на тот компьютер, на котором планируется использование данного сертификата с закрытым ключом. Вставьте носитель закрытого ключа в этот же компьютер и откройте «Панель управления». Найдите там значок «КриптоПро CSP» и дважды щелкните по нему левой кнопкой мыши:



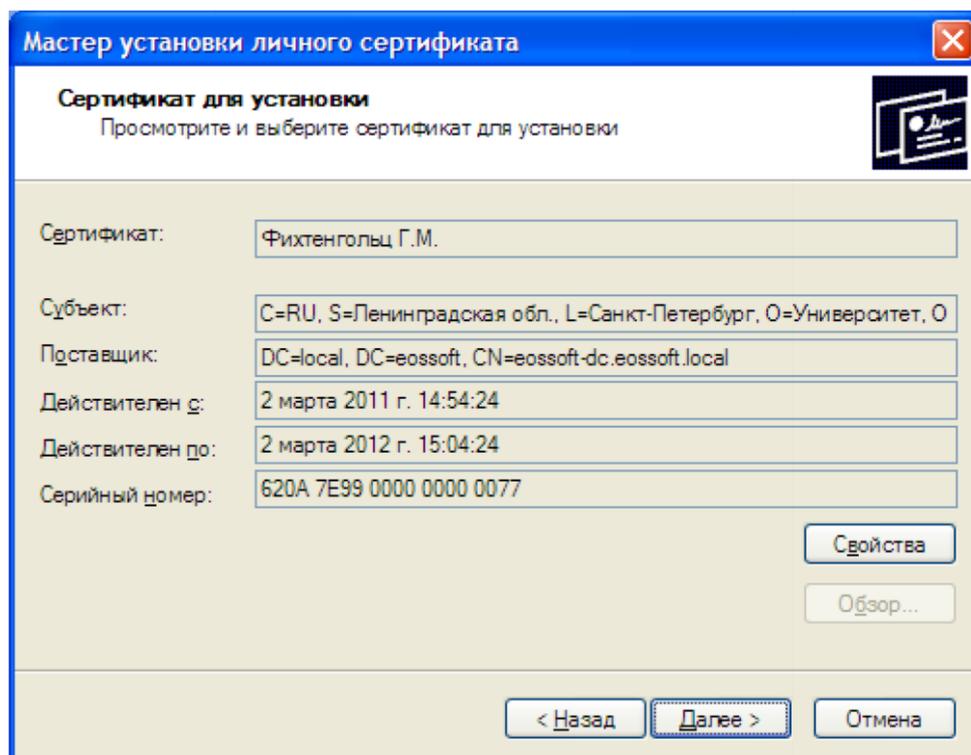
После того, как запустится оснастка КриптоПро, откройте в появившемся окне вкладку «Сервис»:



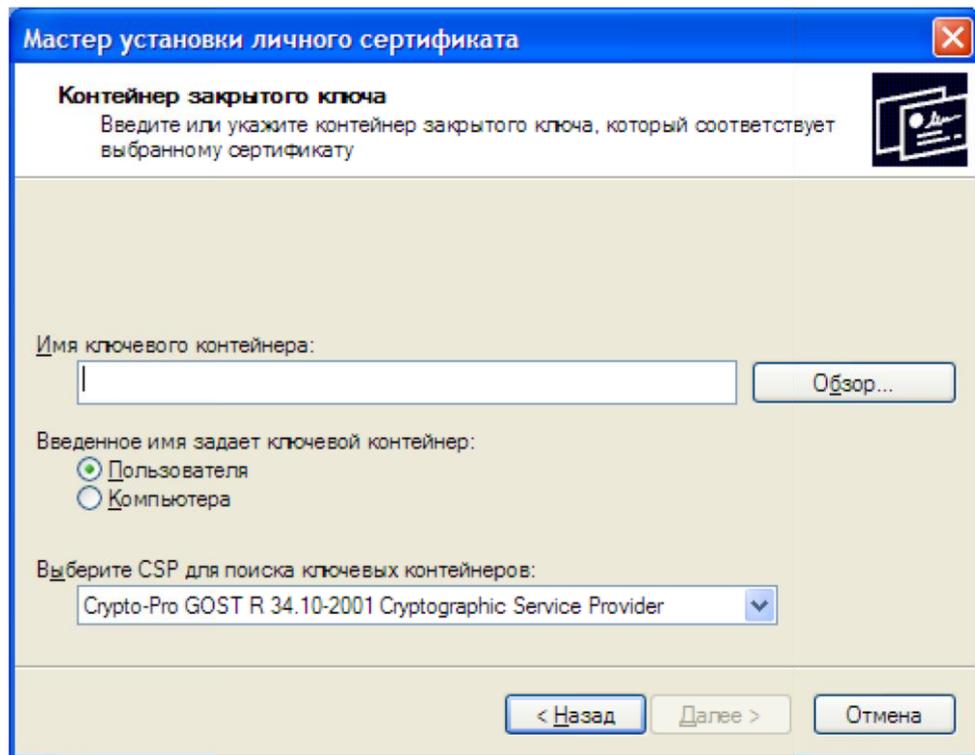
Для начала установки, нажмите на кнопку «Установить личный сертификат» и в появившемся окне мастера нажмите «Далее», после чего Вы увидите следующую страницу мастера:



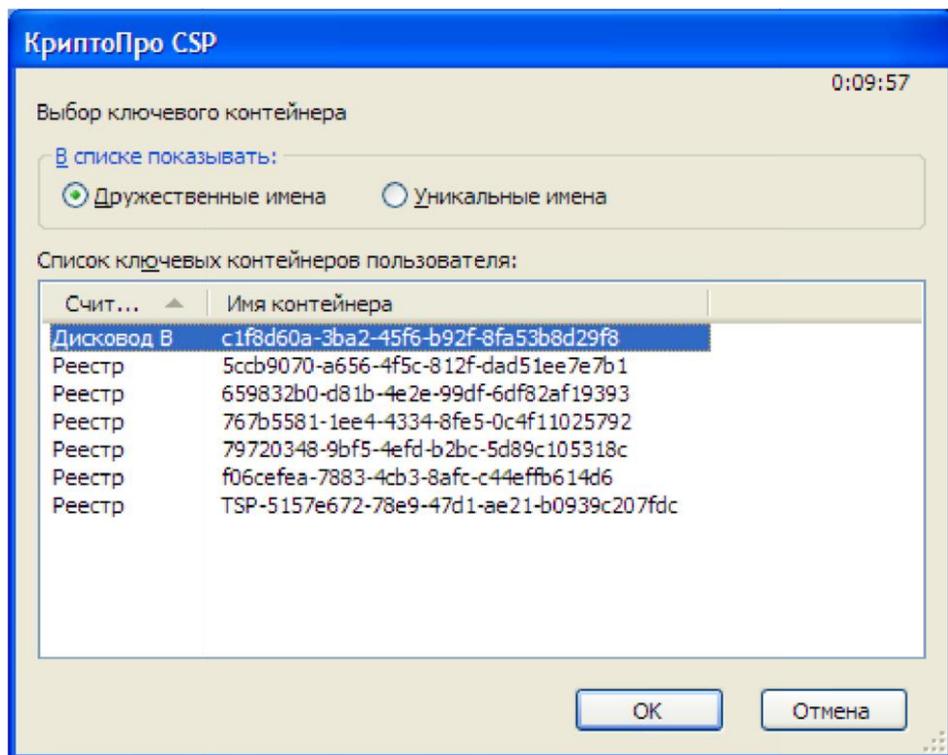
Выберите расположение файла сертификата, который Вы хотите загрузить и нажмите кнопку «Далее». На появившейся странице будет показана подробная информация о содержимом сертификата:



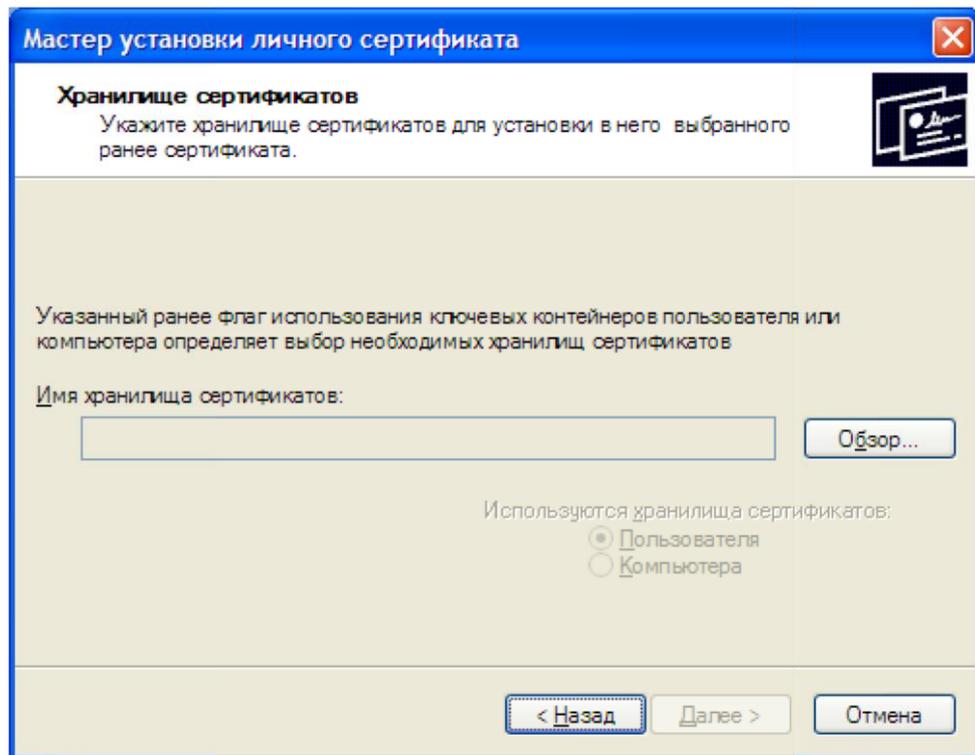
После нажатия кнопки «Далее» Вы увидите страницу выбора соответствующего сертификату ключевого контейнера:



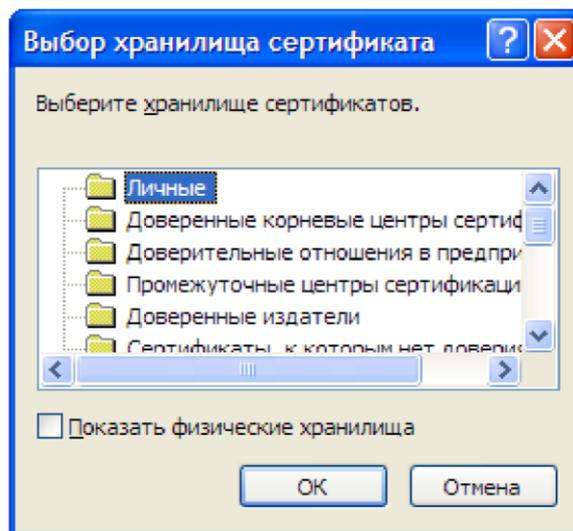
При нажатии на кнопку «Обзор» система предложит выбрать ключевой контейнер из всех доступных в системе для данного криптопровайдера:



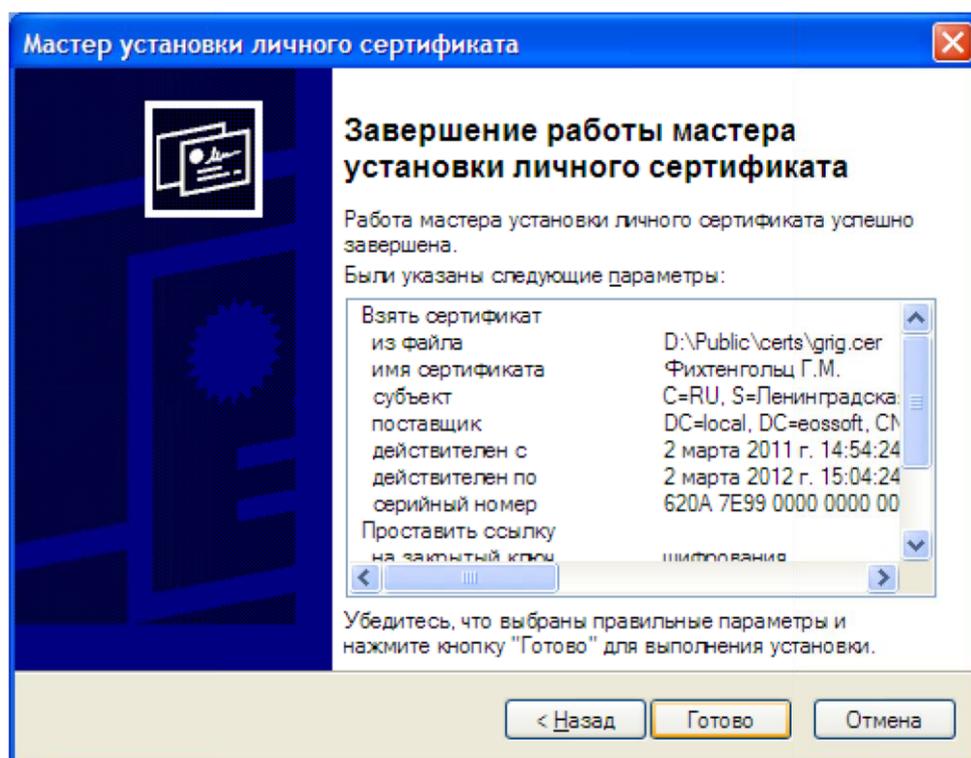
Если ключевой контейнер будет выбран неверно, система выведет соответствующее сообщение об ошибке. Выберите ключевой контейнер и нажмите кнопку «Далее». Вы увидите страницу выбора хранилища сертификатов, в которое следует установить данный сертификат:



При нажатии кнопки «Обзор» выводится список хранилищ для выбранного расположения:



Выберите соответствующее хранилище и нажмите кнопку «Далее». На следующей странице мастера Вы можете просмотреть отчет программы о выполненной операции:



По завершении мастера установки сертификат будет установлен в выбранное хранилище, будет привязан к секретному ключу (что соответствующим образом отображается системой Windows при просмотре списка сертификатов в данном хранилище) и может быть использован для операций шифрования, расшифровывания и создания цифровой подписи.

Работа с корневыми сертификатами

Для того чтобы система могла проверить статус сертификата, а вместе с тем и корректность цифровой подписи, необходимо, чтобы ей был известен статус всех составляющих цепочки данного сертификата. Таким образом, недостаточно установить сам сертификат на компьютер (с закрытым ключом или без него), но требуется также установить всю цепочку данного сертификата до главного корневого сертификата.

Корневой сертификат – это сертификат удостоверяющего центра. С его помощью подписываются все сертификаты, выдаваемые этим удостоверяющим центром. Именно подпись, сделанная с помощью этого сертификата, позволяет говорить о принадлежности пользовательского сертификата и, отчасти, о его статусе (валидности).

Корневой сертификат является, как правило, самоподписанным сертификатом, то есть сертификатом, который удостоверяет целостность самого себя с помощью цифровой подписи. Это означает, что нет возможности проверить его валидность. Соответственно, для осуществления работы с пользовательскими сертификатами, сертификаты удостоверяющих центров необходимо объявить доверенными (при этом необходимо быть уверенным, что данный сертификат действительно является сертификатом соответствующего удостоверяющего центра). Для этого корневые сертификаты устанавливаются в специальное хранилище «Доверенные корневые центры сертификации», и система принимает их как валидные.

Корневой сертификат может быть не самоподписанным, более того, их может быть несколько, следующих друг за другом в цепочке. Это возможно в том случае, если один удостоверяющий

центр (например, более высокий по статусу) выдает сертификат с правом выдачи (подписания) сертификатов другому удостоверяющему центру. В таком случае эти сертификаты недостаточно установить в «Доверенные корневые центры сертификации», необходимо также, чтобы там находились все сертификаты, присутствующие в цепочке выше проверяемого, включая исходный корневой самоподписанный сертификат.

Так как для работы с цифровыми подписями требуется полная цепочка сертификатов и, в особенности, корневые, рассмотрим момент установки корневого сертификата подробнее.

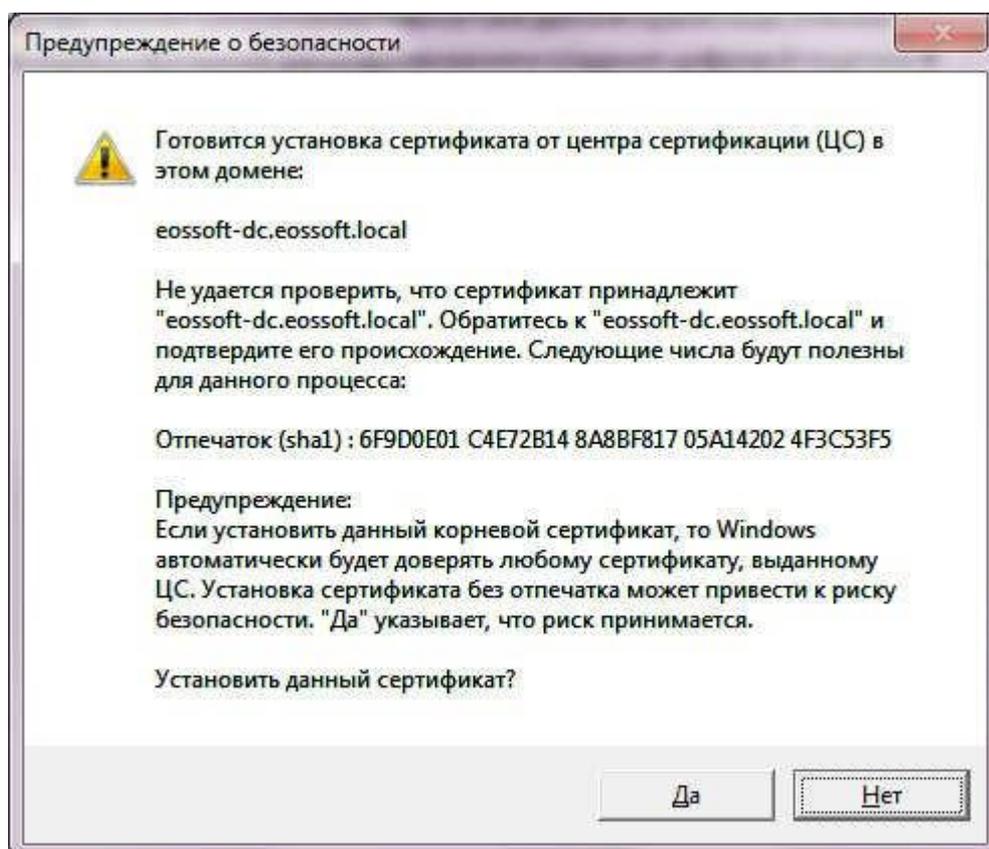
В целом, корневой сертификат, так же как и пользовательский, может быть установлен в автоматическом режиме, однако в данном случае возникает проблема с видимостью данного сертификата. Дело в том, что автоматически сертификат будет установлен в хранилище «Доверительные отношения в предприятии» и в хранилища текущего пользователя.

При установке в это хранилище сертификат не становится доверенным (для чего следует установить его в «Доверенные корневые центры сертификации»), кроме того, хранилища текущего пользователя доступны приложениям и системе только в том случае, если текущий пользователь вошел в систему. Такой режим крайне неудобен, если Вы хотите, чтобы информацией из хранилища пользовалась, к примеру, системная служба (так как системные службы запускаются до входа пользователя в систему и не требуют его). Для того, чтобы все приложения, работающие на компьютере (в том числе и системные службы) могли обнаружить данный корневой сертификат, следует произвести установку в хранилище «Доверенные корневые центры сертификации» локального компьютера (более подробно установка сертификатов в хранилища описана в соответствующем пункте).

Внимание! Некоторые системные службы берут корневые сертификаты непосредственно из хранилища «Доверенные корневые центры сертификации» службы. Для корректной работы таких служб следует устанавливать сертификат как в хранилище локального компьютера, так и данной службы.

Во избежание проблем, которые могут возникнуть в ходе работы различных приложений с корневыми сертификатами, рекомендуется устанавливать их как в хранилище текущего пользователя (либо системной службы, если работа с сертификатами планируется с ее помощью), так и в хранилище локального компьютера (для всех). Это связано с тем, что некоторые приложения могут искать корневые сертификаты только в собственных, принадлежащих пользователю или приложению, хранилищах.

Процесс установки сертификата в данные хранилища отличается от установки в любое другое тем, что в процессе установки Вы, перед непосредственным импортом сертификата, можете увидеть следующее информационное окно с вопросом:



Данное окно призвано защитить Вас от автоматической установки сертификатов приложениями, находящимися на данном компьютере, среди которых могут быть недоверенные. Если Вы уверены, что именно этот сертификат Вы хотите назвать доверенным, нажмите «Да», после чего процесс импорта сертификата будет завершен. Данное окно не появится том случае, если с компьютера, на который осуществляется установка, есть сетевой доступ к удостоверяющему центру, которому, предположительно, принадлежит данный корневой сертификат, и удостоверяющий центр подтверждает его принадлежность и валидность. Если же такой связи нет, то информацию, показанная в данном окне (в частности, имя домена и отпечаток (sha1)) следует отправить в удостоверяющий центр, и не продолжать установку до получения положительного ответа о принадлежности сертификата.

Все пользовательские сертификаты, подписанные с помощью данного корневого сертификата, с этого момента не будут признаваться недействительными на основании отсутствия корневого сертификата.