

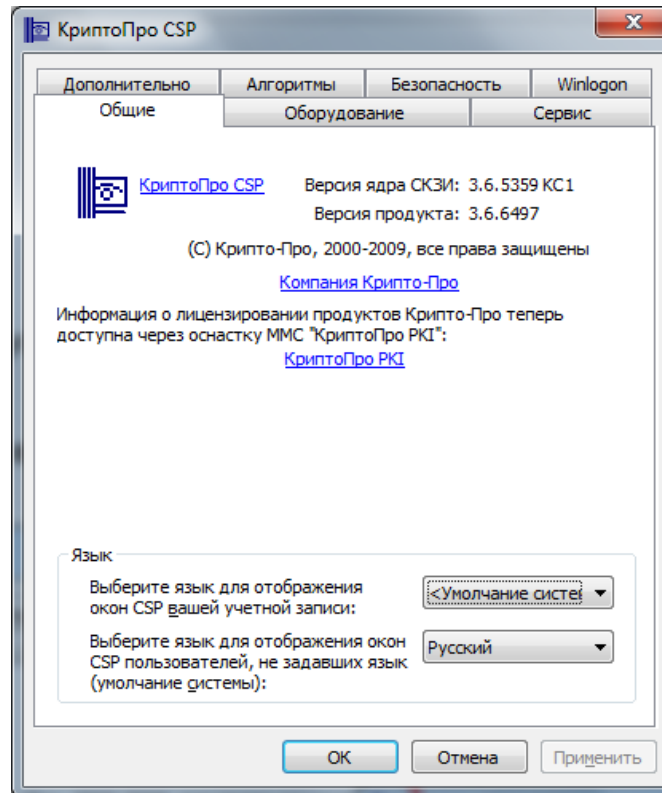
На данный момент можно выбрать несколько удостоверяющих центров, аккредитованных на территории Магаданской области :

- 1. ООО ОП «Русь-Телеком»**, г. Магадан, ул. Советская, д. 2, тел.: (4132) 60-88-48,
<http://www.rus-telecom.ru>
- 2. ОАО «Датаком»**, г. Магадан, ул. Советская, д. 5, тел.: (4132) 60-8888,
<http://www.dtcom.ru>
- 3. ООО «МАГТЕЛ»**, г. Магадан, Якутская, д.71, тел.(4132) 200-200,
<http://www.maglan.ru/pki>

! Необходимо заказать у выбранного Удостоверяющего Центра ЭЦП для работы с электронной системой отчетности ЕИАС Мониторинг

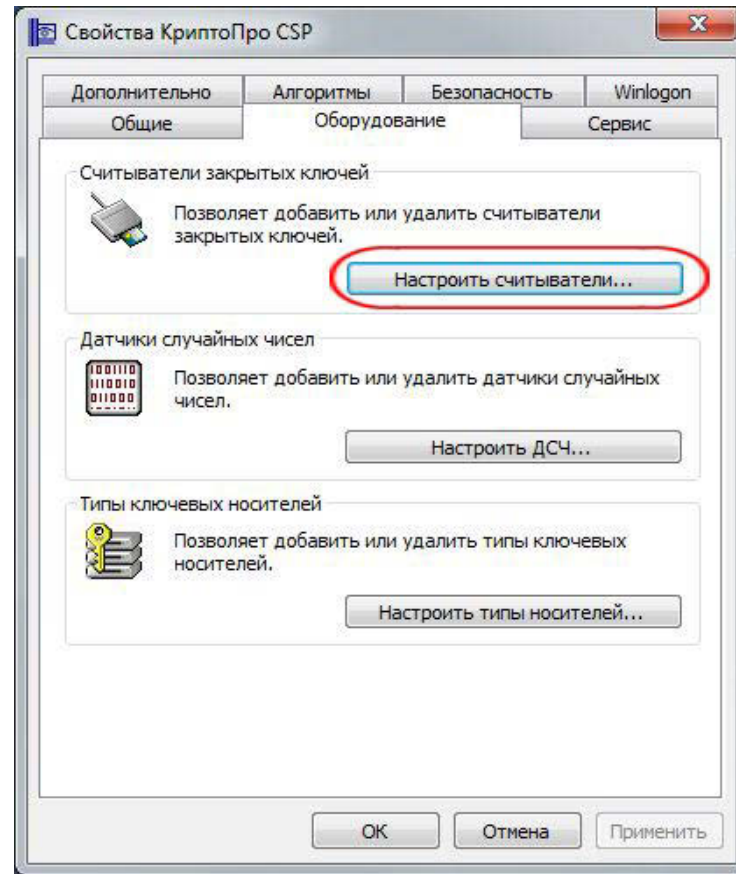
Шаг 2. Установка личного сертификата электронно-цифровой подписи на компьютер

1. Установите программу **Крипто-ПРО**, указав **ключ лицензии***, а также драйверы для работы с защищенным носителем **RuToken** (при его использовании), по завершении установки обязательно перезагрузить компьютер.
2. После перезагрузки компьютера через меню **Пуск - Все программы – Крипто-ПРО**, либо через **Панель управления** запустите **КриптоПРО CSP**



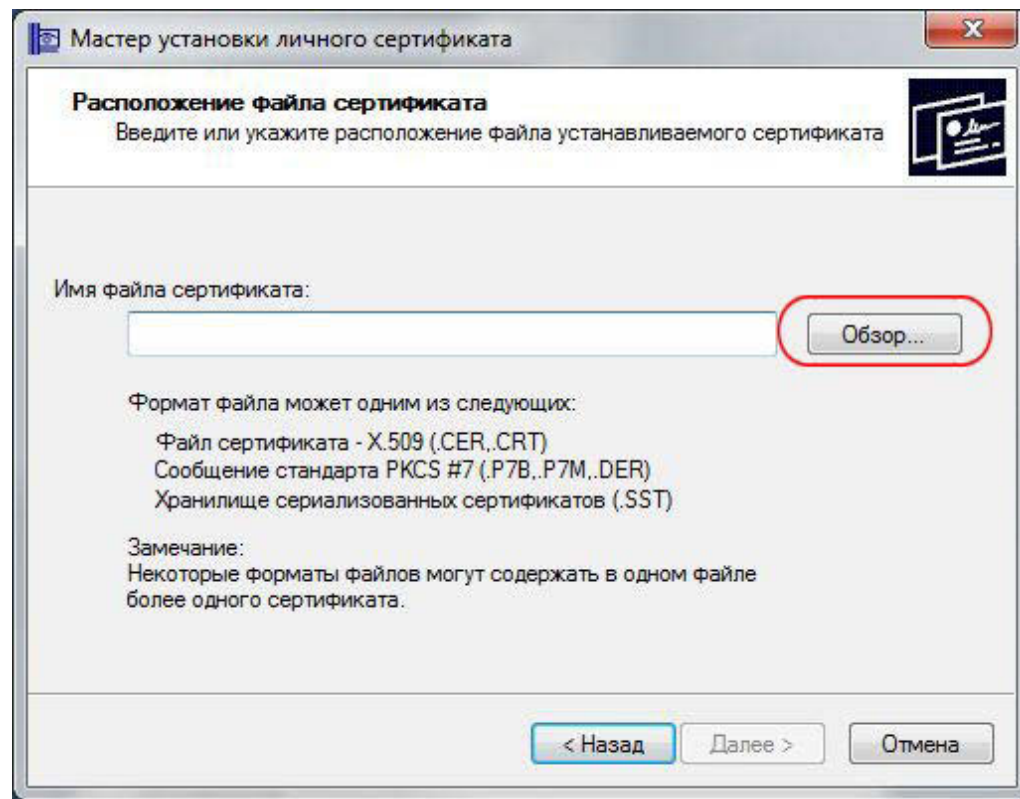
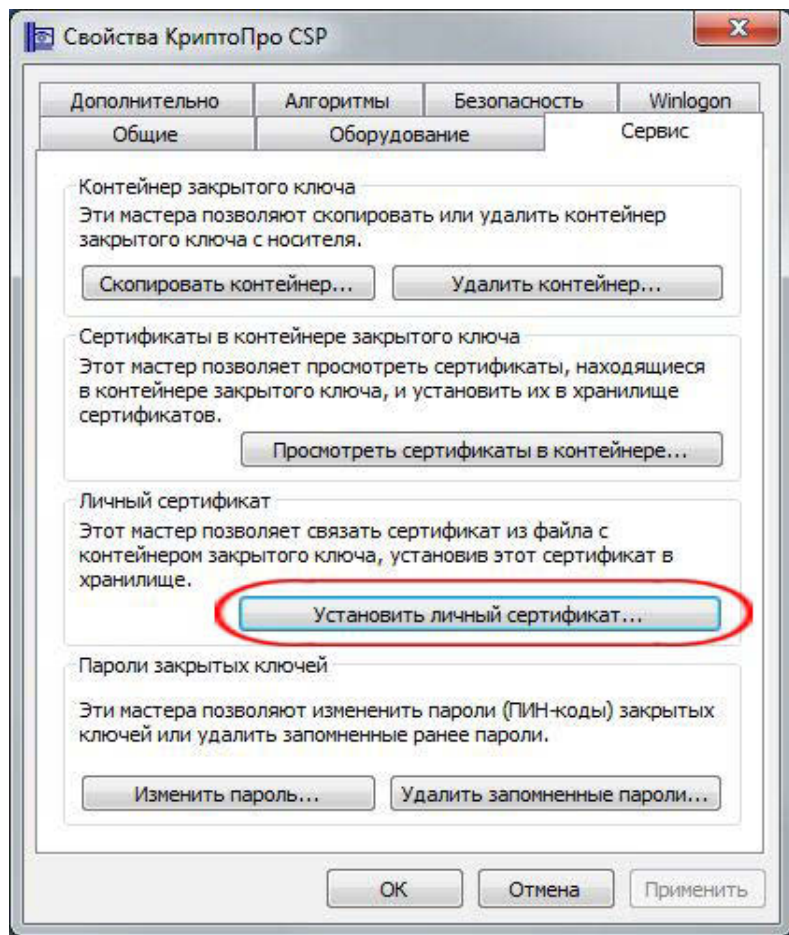
** Программу Крипто-ПРО и лицензию на ее использование можно приобрести в Удостоверяющем центре сертификации вместе с личным сертификатом ЭЦП. Для Windows Vista и Windows 7 необходима версия 3.6 !*

3. Для добавления устройства (носителя, считывателя), на котором у вас хранится контейнер ЭЦП*, переключитесь на вкладку **Оборудование**, кнопка **Настроить считыватели**.



**Контейнер – это закрытая часть ключа ЭЦП. Контейнер ключа может храниться на считывателях: защищенном носителе RuToken/EToken, на съемных дисках – дисководы (дискета, флешка).*

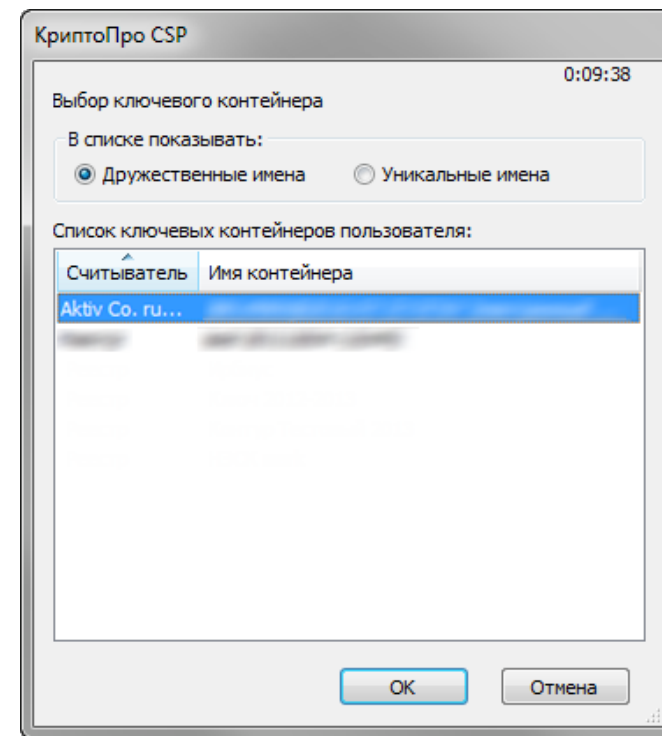
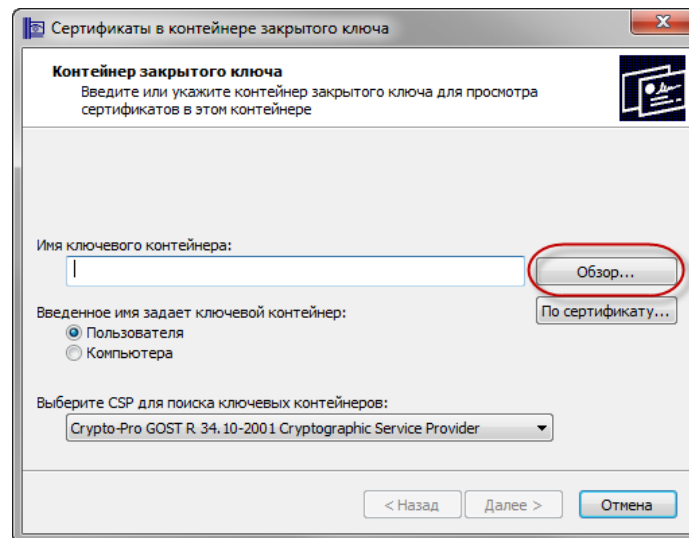
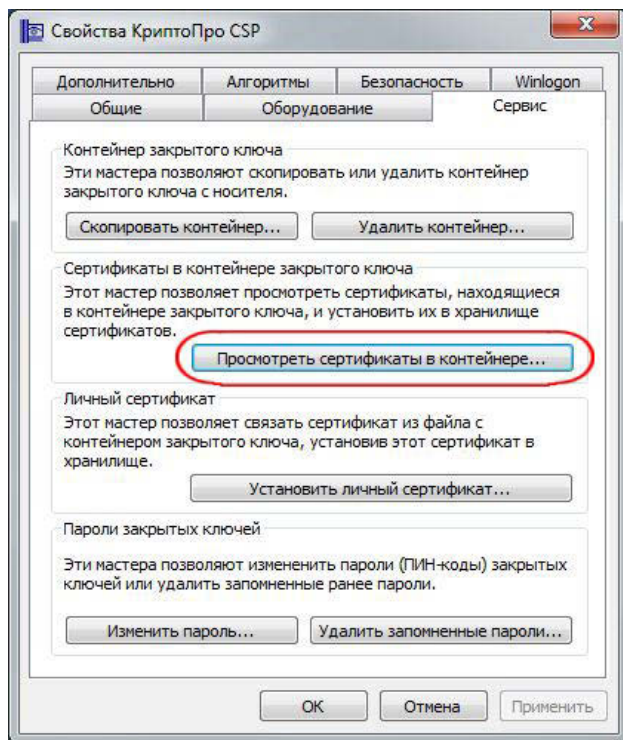
4. Переключитесь на вкладку **Сервис** и нажмите кнопку **Установить личный сертификат**.
Запустится **Мастер установки личного сертификата**.
5. По кнопке **Обзор** выберите файл сертификата (файл открытого ключа с расширением **.cer**).



6. Выгрузка сертификата открытого ключа (в случае его отсутствия)

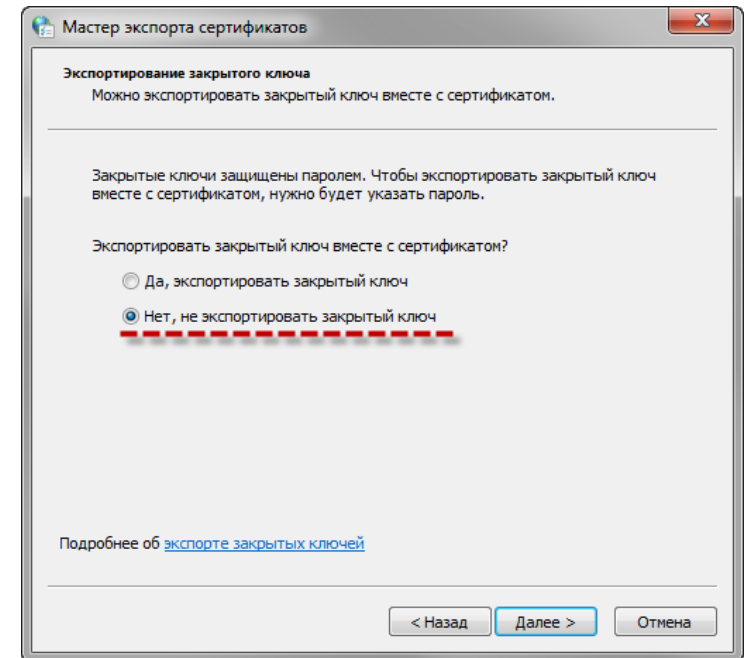
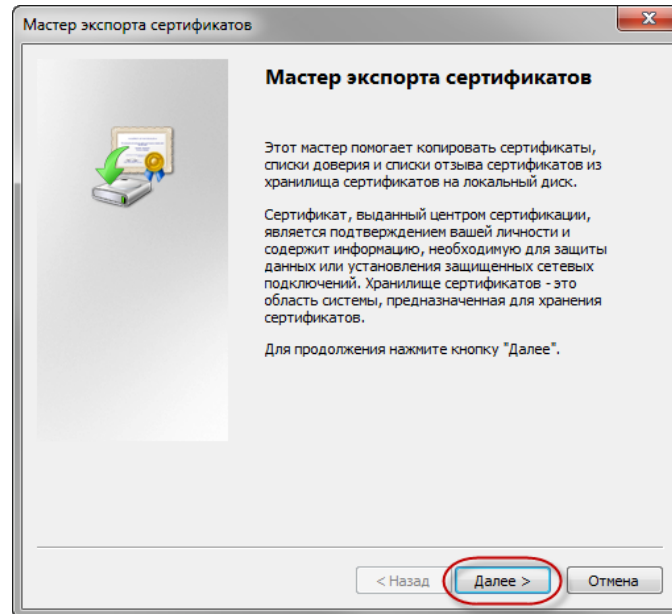
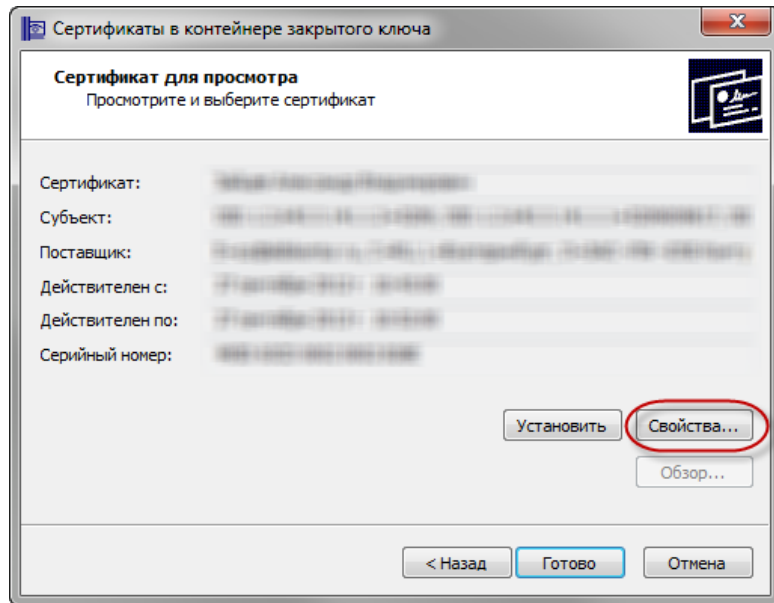
ЭЦП состоит из закрытого ключа и открытого ключа (сертификат .cer) Удостоверяющие центры выдают ЭЦП на ключевых носителях - РуТокен/ЕТокен, флэш-накопитель. Если у вас флэш-накопитель, то в корне носителя должен быть файл с расширением .cer - сертификат безопасности. Если у вас защищенный ключевой носитель РуТокен/ЕТокен, то физически увидеть вы его не можете. **Для этого открытый ключ необходимо экспортировать.**

Это можно сделать с помощью программы **Крипто-ПРО** нажав вкладку **Сервис** и кнопку **Посмотреть сертификат** в контейнере, далее **Обзор** – выбрать носитель и контейнер на нем, нажмите **ОК**



В случае наличия файла открытого ключа в контейнере закрытого ключа, система отобразит окно с информации о нем.

Нажмите кнопку **Свойства**. В открывшемся окне свойств сертификата перейти на вкладку **Состав** и нажать кнопку **Копировать в файл**, запустится **Мастер импорта сертификатов**. Ответьте на вопросы мастера: – **Нет, не экспортировать закрытый ключ** – **Далее**

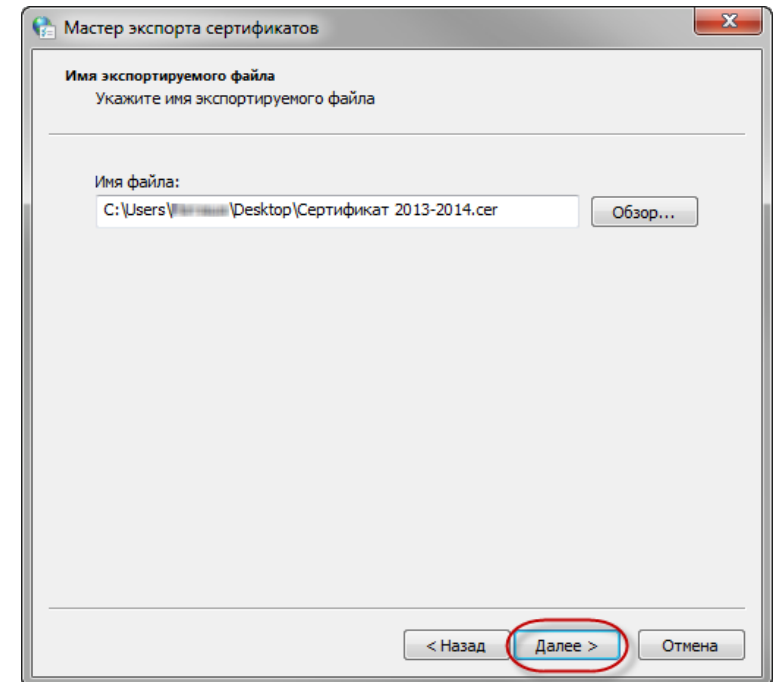
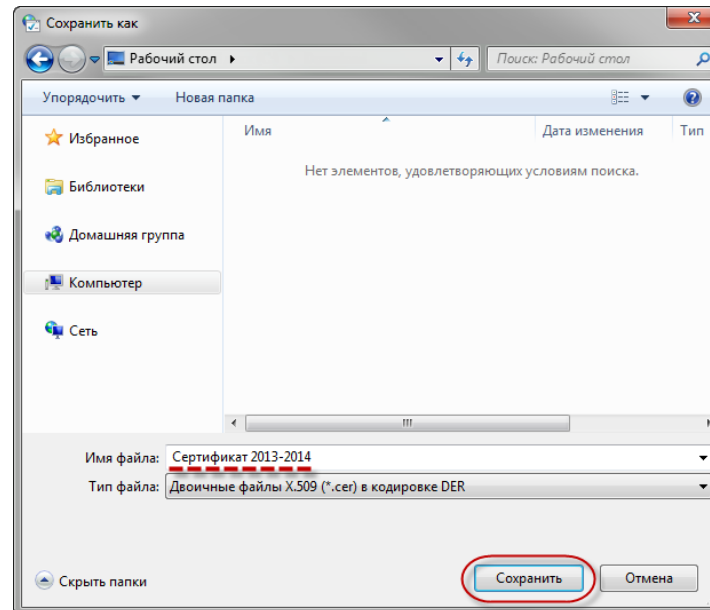
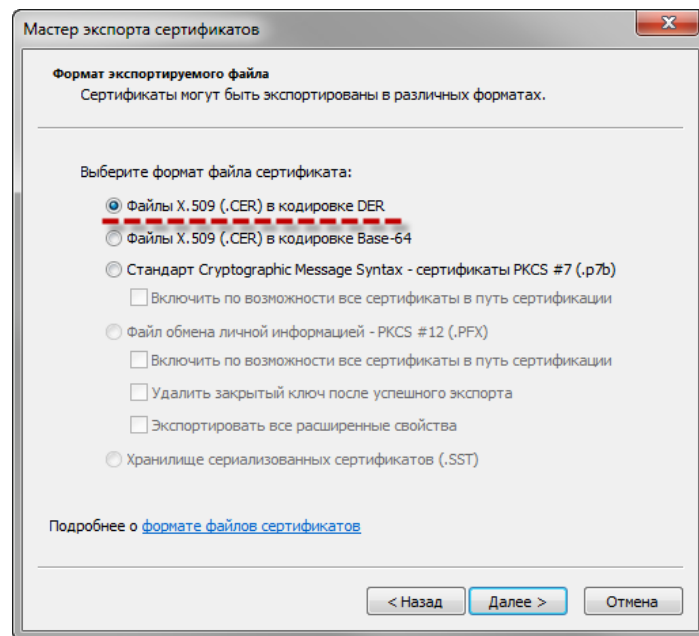


выбираем - **Файлы X.509 (.CER)** в кодировке DER – **Далее**

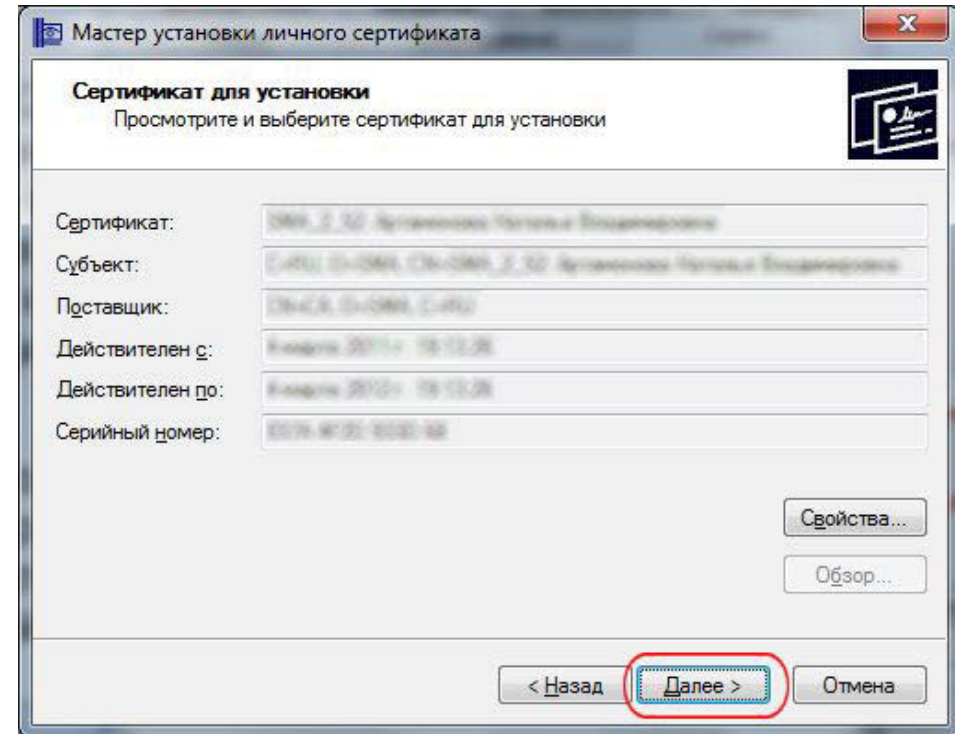
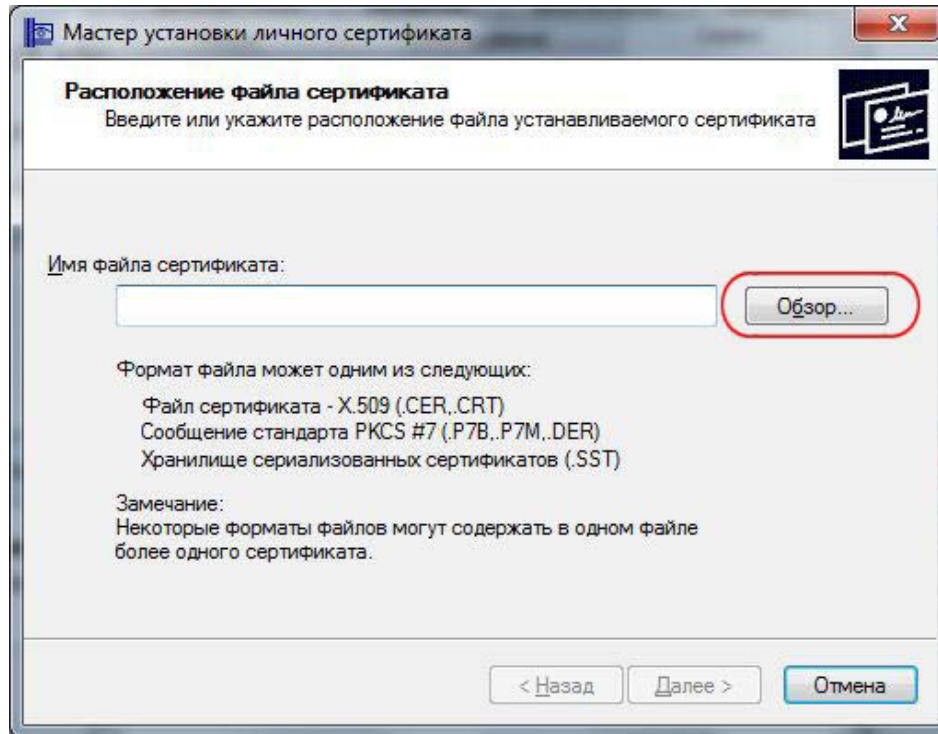
выберите папку, куда необходимо сохранить файл (в этом окне внизу укажите желаемое имя файла). **Сохранить** – **Далее** – **Готово**.

Мастер импорта сертификатов завершит свою работу.

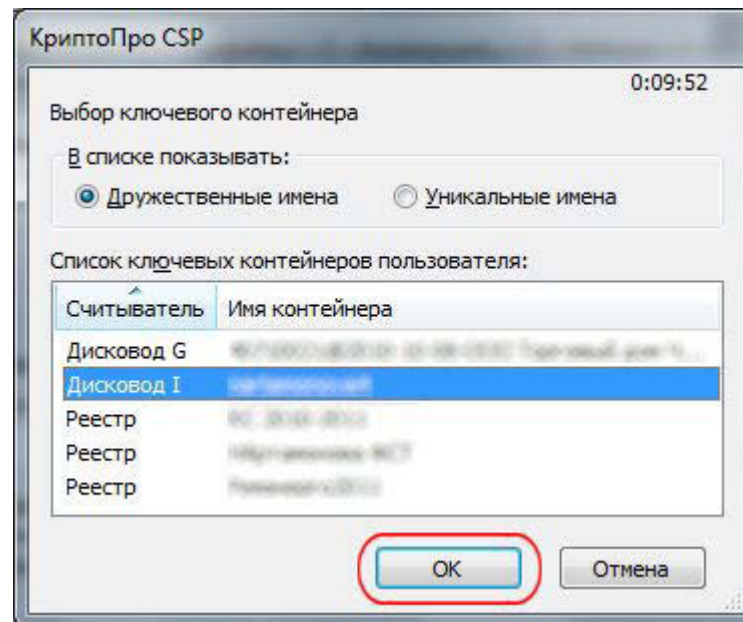
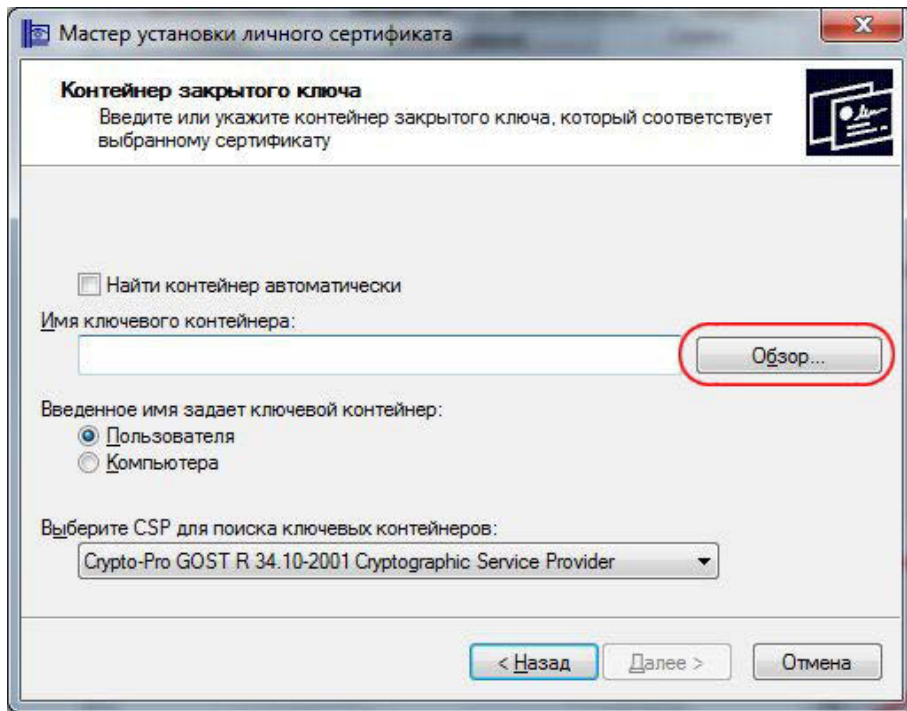
В результате этих действий в указанной вами папке **создается открытый файл сертификата ключа ЭЦП**.



7. После выбора файла сертификата (файла открытого ключа с расширением .cer).
В окне **Сертификат для установки** отображаются краткие сведения об устанавливаемом сертификате.
Переходим **Далее**.

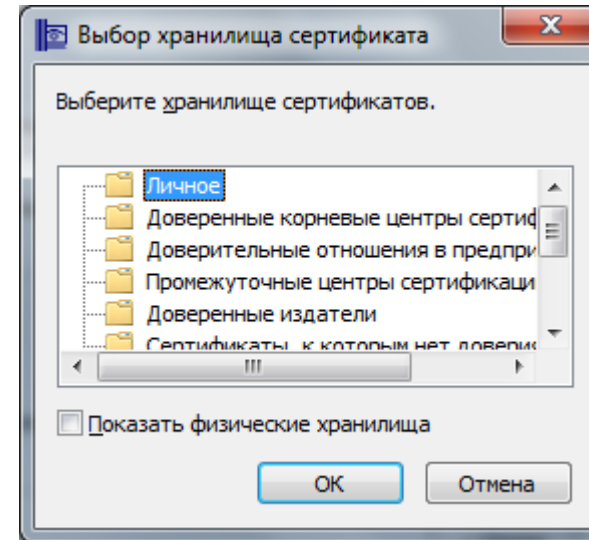
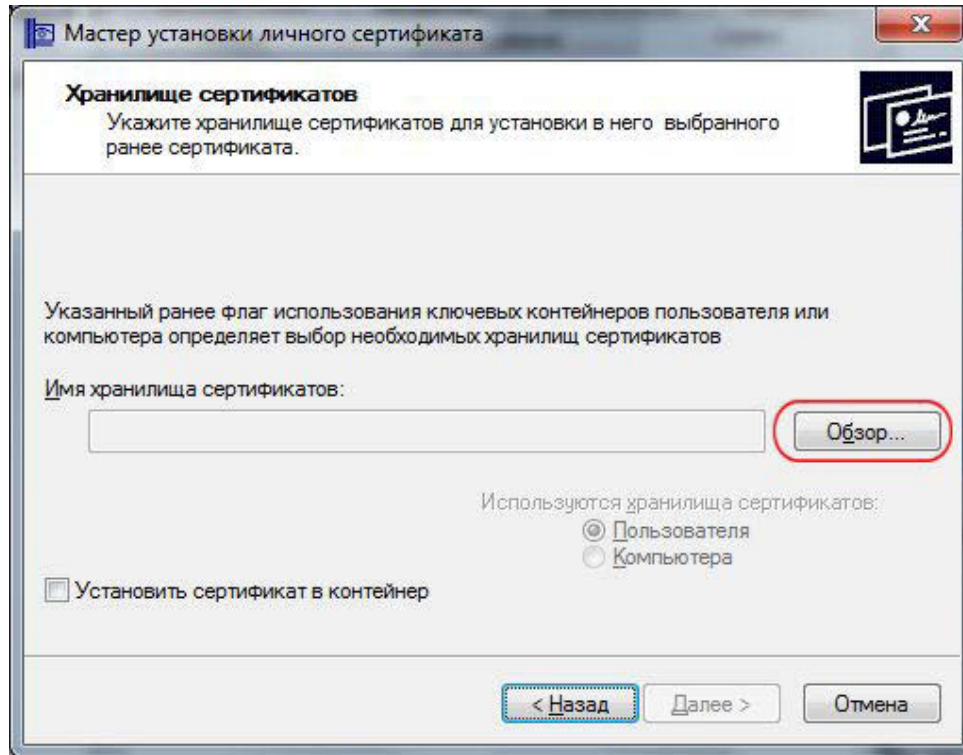


8. В следующем окне необходимо указать контейнер закрытого ключа. Нажимаем на кнопку **Обзор** и в открывшемся небольшом окне выбираем нужный считыватель и контейнер закрытого ключа на нем.

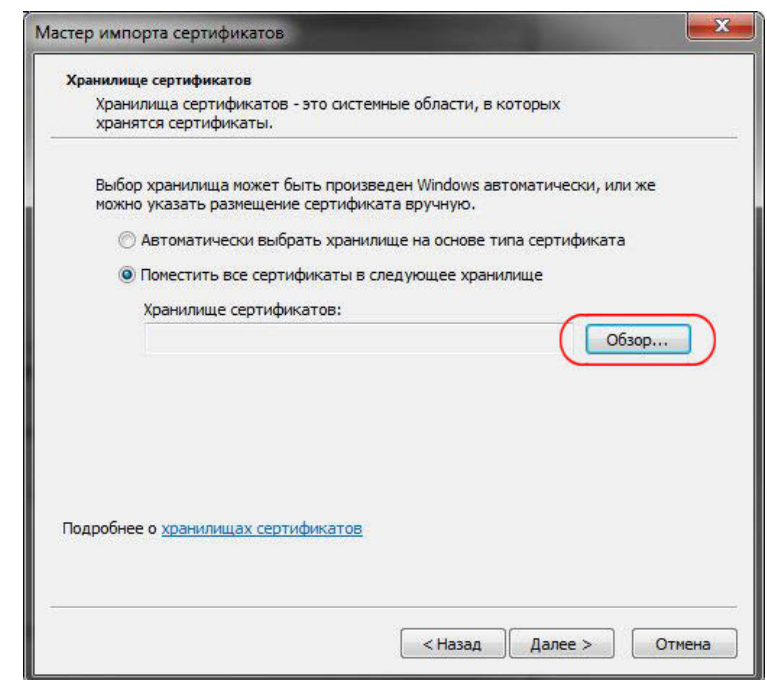
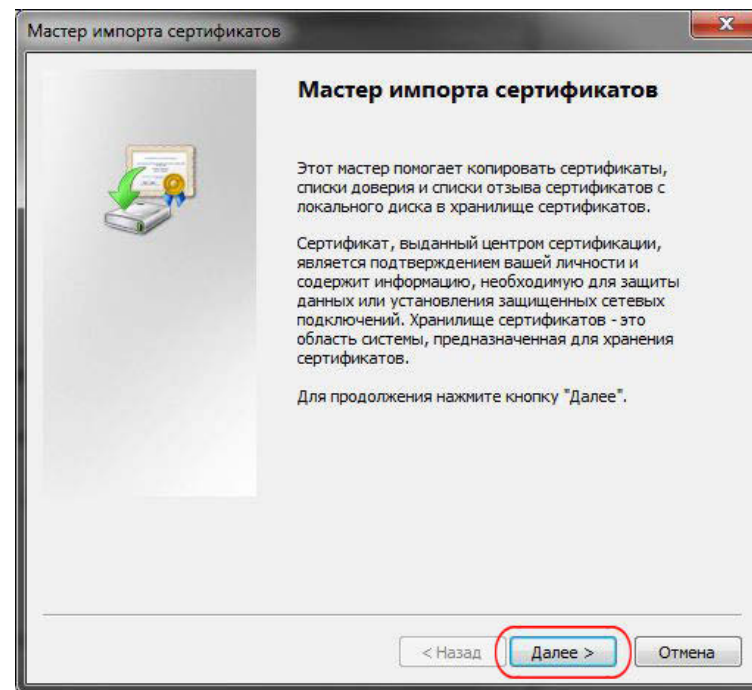
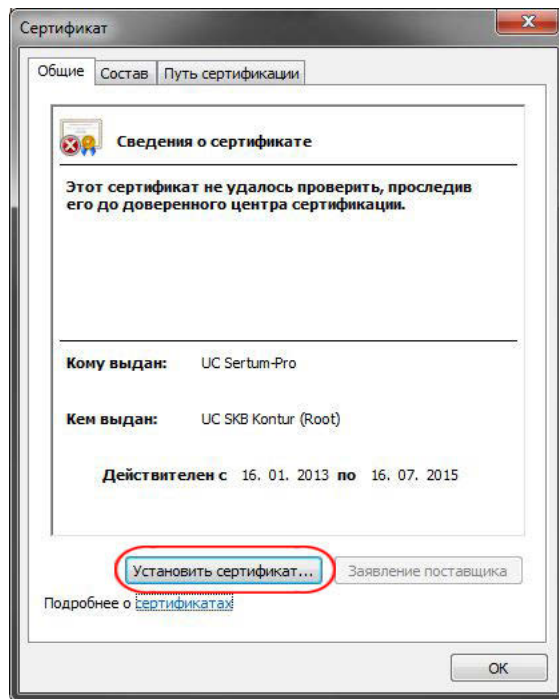


Важно! Все привязки закрытого и открытого ключей должны быть выполнены для **текущего пользователя**, а не для локального компьютера. Таким образом в блоке **Введенное имя задает ключевой контейнер** всегда должен выбран параметр **Пользователя**.

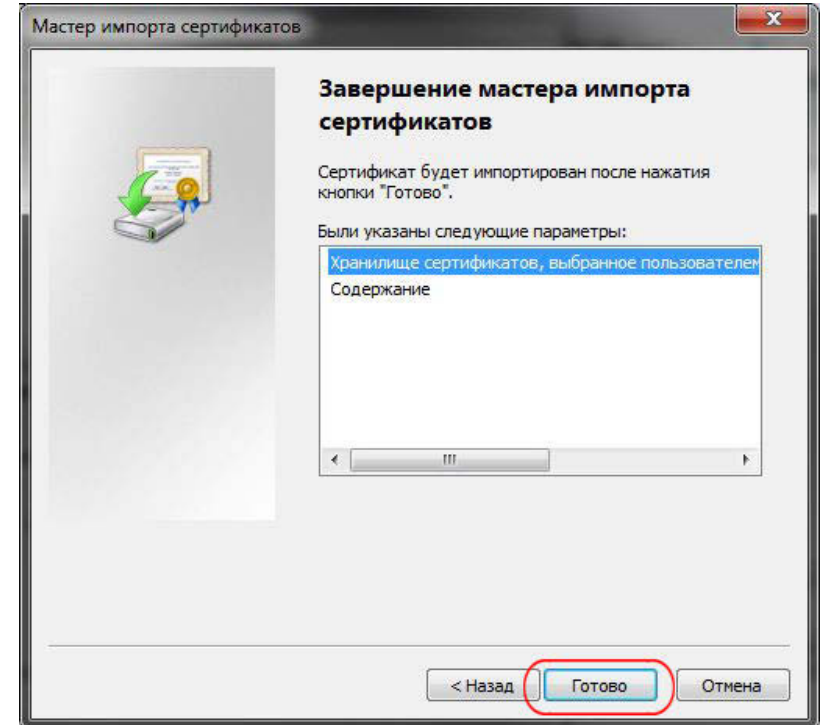
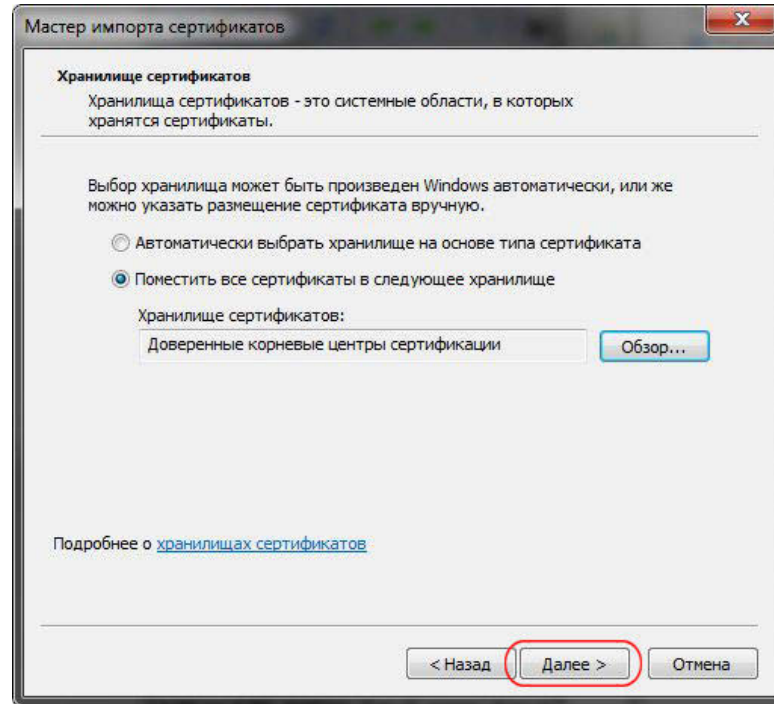
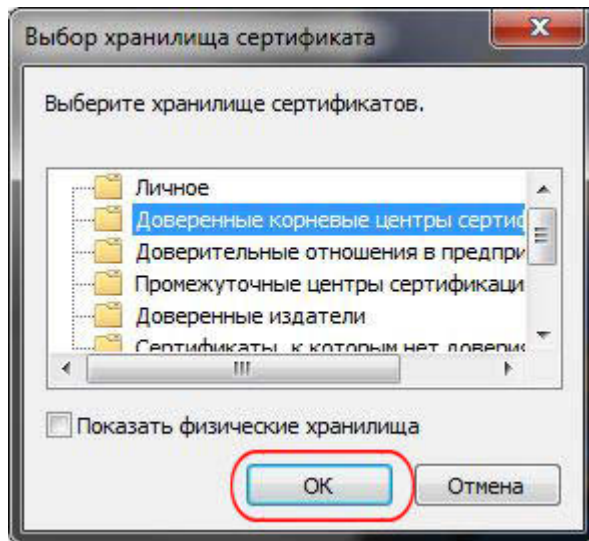
9. Далее по кнопке **Обзор** необходимо указать хранилище, в которое будет помещен сертификат. Все сертификаты пользователя должны быть помещены в хранилище сертификатов **Личное**. На завершающем этапе **Мастер установки личного сертификата** сообщит об успешном завершении установки сертификата электронно-цифровой подписи.



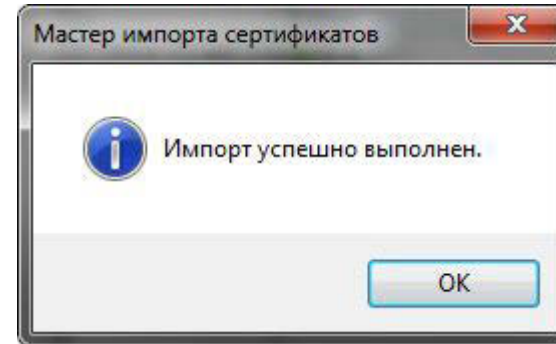
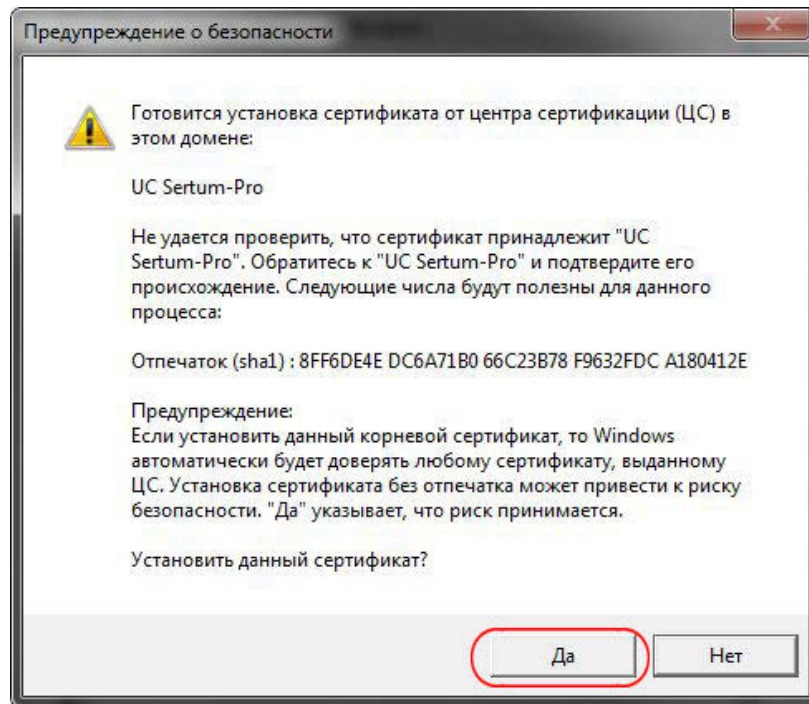
10. После установки личного сертификата необходимо установить **доверенный корневой сертификат**.
Корневой сертификат можно получить вместе с личным сертификатом в **Удостоверяющем центре**, либо скачать в **Корневом центре сертификации** <http://ca.sertum.ru/certificates/> файл сертификата [sertum-pro-qualified-2013.cer](http://ca.sertum.ru/certificates/sertum-pro-qualified-2013.cer), либо другие корневые сертификаты по адресу <http://ca.skbkontur.ru/about/certificates> .
Для установки сертификата надо **кликнуть на файл самого сертификата**, после этого появится окно с просмотром свойств сертификата, в котором нажать кнопку **Установить сертификат**, запустится **Мастер импорта сертификатов**, нажать **Далее**, в появившемся окне выбрать раздел **Поместить все сертификаты в следующее хранилище** и нажать кнопку **Обзор**



В окне **Выбор хранилища сертификата** выбрать раздел **Доверенные корневые центры сертификации** и нажать **ОК**, после выбора хранилища нажать кнопку **Далее**, в следующем окне нажать кнопку **Готово** для завершения работы **Мастера импорта сертификатов**.



Появится предупреждение о безопасности с предложением «Установить данный сертификат?»
Нажать **Да** , следующее окно проинформирует **об успешном импорте сертификата**



11. Далее нужно запустить обозреватель **Internet Explorer** и зайти в раздел **Сервис - Свойства обозревателя**, перейти на закладку **Содержание** и нажать на **Сертификаты**.
При правильной установке, **личный и корневой сертификаты** должны отображаться, как показано на рисунке.

