Установка сертификатов и списка отозванных сертификатов

17.10.2014

Национальный удостоверяющий центр
Луковников Д.А., Бойков Л.В.

Содержание

1. Введение

В данном документе описан порядок установки личного сертификата и корневых сертификатов, выпущенных удостоверяющим центром ЗАО «Национальный удостоверяющий центр».

Перед установкой сертификатов необходимо, предварительно установить программное обеспечение КриптоПро CSP (см. раздел 2) и драйверы ключевого носителя, на котором был выпущен Ваш сертификат.

2. Установка КриптоПро CSP

Для компьютеров под управлением операционных систем семейства Windows, начиная с Windows XP и по Windows 8 включительно, рекомендуется устанавливать КриптоПро CSP 3.6 R4. Для компьютеров под управлением операционной системы Windows 8.1 рекомендуется устанавливать КриптоПро CSP 3.9.

Дистрибутив КриптоПро CSP необходимо скачать с сайта производителя http://www.cryptopro.ru/products/csp/downloads.

Для того, что бы установить КриптоПро CSP запустите установочный пакет и следуйте подсказкам мастера установки. Подробную инструкцию по установке и использованию КриптоПро CSP см. в документе «Инструкция по использованию КриптоПро CSP», скачать которую вы можете в разделе «Документация» на сайте производителя (http://www.cryptopro.ru/support/docs).

3. Установка драйверов ключевого носителя Рутокен

Если в качестве ключевого носителя при выпуске сертификата использовался Рутокен, то необходимо скачать и произвести установку драйверов Рутокен. В зависимости от типа операционной системы (32-х или 64-х бит), необходимо скачать соответствующий дистрибутив из раздела «Загрузки» с сайта производителя http://www.rutoken.ru/support/download/drivers-for-windows/.

Для того, что бы установить драйверы запустите установочный пакет и следуйте подсказкам мастера установки. В случае необходимости, может потребоваться перезагрузка компьютера. Подробную инструкцию по установке драйверов и использованию Рутокен см. в документе «Инструкция по настройке и использованию Рутокен», скачать которую вы можете в разделе «Документация» (http://www.rutoken.ru/support/download/manual/) на сайте производителя.

4. Установка драйверов ключевого носителя eToken

Если в качестве ключевого носителя при выпуске сертификата использовался eToken, то необходимо скачать и произвести установку драйверов eToken. Архив с дистрибутивом необходимо скачать из раздела «Цент загрузки» с сайта производителя http://www.aladdin-rd.ru/support/downloads/26037/.

Подробную инструкцию по установке драйверов eToken см. в документе «eToken PKI Client 5.1 SP1. Руководство администратора» в архиве дистрибутива.

5. Установка драйверов ключевого носителя eSmart

Если в качестве ключевого носителя при выпуске сертификата использовался eSmart, то необходимо скачать и произвести установку драйверов eSmart. Архив с дистрибутивом необходимо скачать из раздела «Загрузки» с сайта производителя http://www.esmart.ru/download/. Рекомендуем к установке комплект «ESMART PKI Client для Windows».

Подробную инструкцию по установке драйверов eSmart см. в документе «eSMART PKI Client - Руководство администратора» http://www.esmart.ru/download/.

6. Установка корневых сертификатов Национального удостоверяющего центра

Сертификаты и списки отозванных сертификатов публикуются на сайте Удостоверяющего центра по адресу http://www.nucrf.ru в разделе **«Сертификаты УЦ»**.

Для начала работы необходимо скачать корневые сертификаты Удостоверяющего Центра. Если сертификат владельца выпущен в период с 05.07.2012 по 26.06.2014, то необходимо скачать сертификат **ncarf-v00.cer.** Если сертификат владельца выпущен в период с 27.06.2014 то необходимо скачать сертификат **ncarf-v01.cer.**

ВНИМАНИЕ! Запомните место, куда Вы сохранили файлы!

Для установки сертификата Удостоверяющего центра **ncarf-v00.cer** или **ncarf-v01.cer** необходимо открыть в Проводнике папку, куда был сохранен файл **ncarf-v00.cer** или **ncarf-v01.cer**, и по нажатию правой кнопки мыши на файле **ncarf-v00.cer** или **ncarf-v01.cer** в контекстном меню выбрать пункт **«Установить сертификат»**. (См. Рис. 6.1)

Рис.6.1. Запуск установки сертификата

В результате выполненных действий откроется страница приветствия **«Мастера импорта сертификатов»**. В этом окне необходимо нажать кнопку **«Далее»** (См. Рис. 6.2):

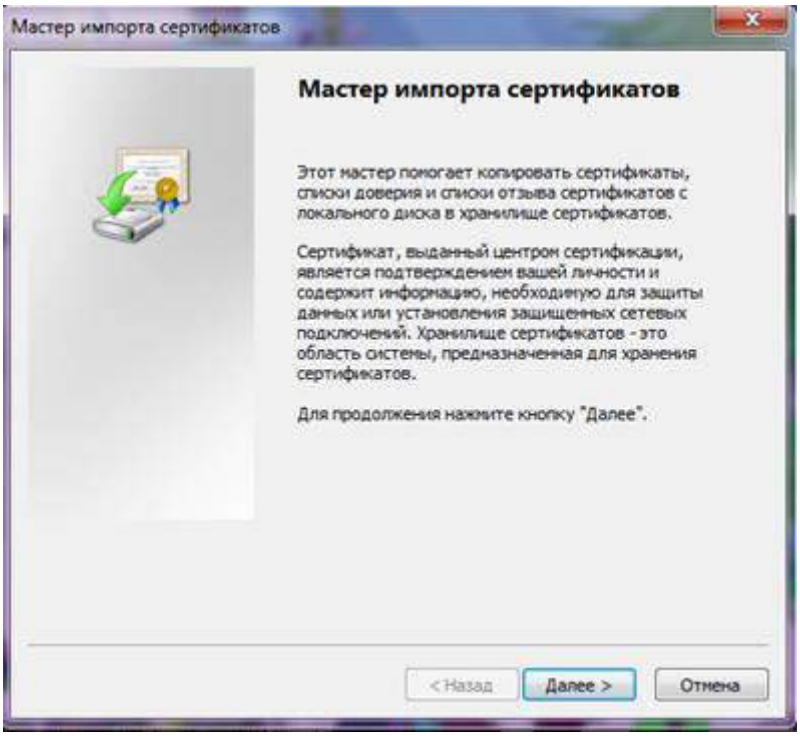

Рис. 6.2. Окно приветствия мастера импорта сертификатов

Откроется страница **«Хранилище сертификатов»**. На этой странице необходимо установить переключатель в позицию **«Поместить все сертификаты в следующее хранилище»** и затем нажать кнопку **«Обзор»** (См. Рис. 6.3):

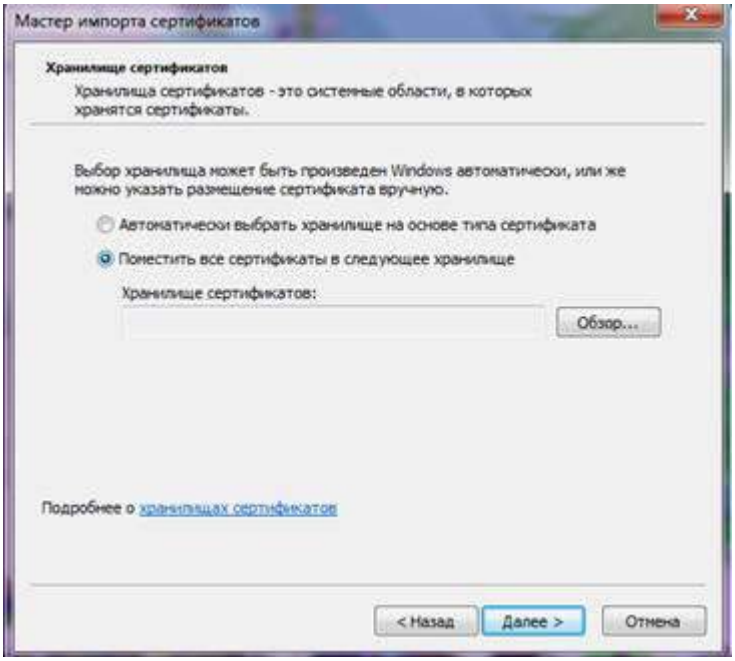

Рис. 6.3. Хранилище сертификатов

Откроется окно **«Выбор хранилища сертификата»**. В этом окне необходимо выбрать хранилище **«Доверенные корневые центры сертификации»** и нажать кнопку **«ОК»** (См. Рис. 6.4):

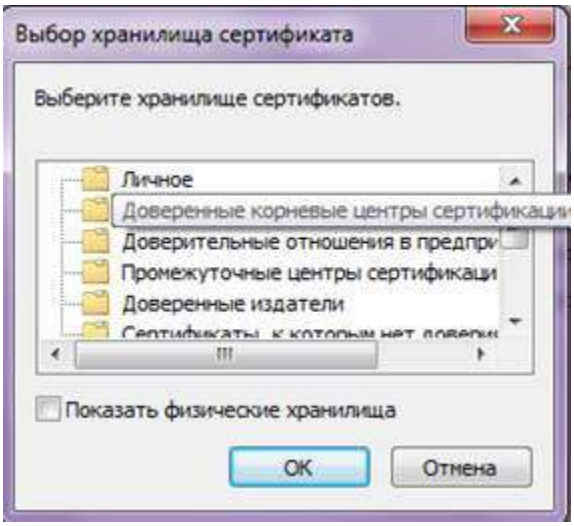

Рис. 6.4. Выбор хранилища сертификата

Окно **«Выбор хранилища сертификата»** закроется. Мастер установки сертификатов вернется на страницу **«Хранилище сертификатов»**. Необходимо нажать кнопку **«Далее»**. Мастер установки сертификатов перейдет на страницу **«Завершение мастера импорта сертификатов».** Необходимо нажать кнопку **«Готово»** (См. Рис. 6.5):

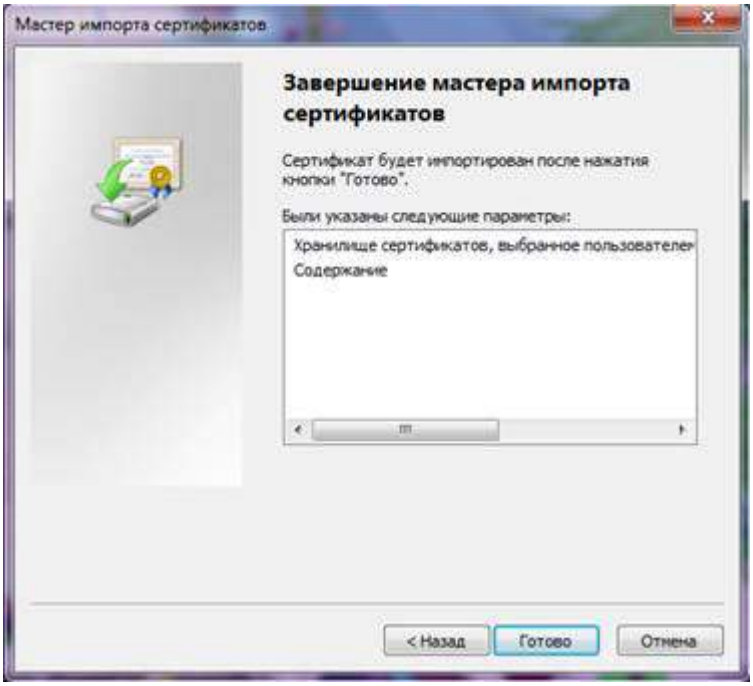

Рис. 6.5. Завершение мастера импорта сертификатов

В некоторых случаях может появиться предупреждение системы безопасности о том, что готовится сертификата от центра сертификации Национального удостоверяющего центра. На вопрос о том, следует ли установить сертификат необходимо ответить утвердительно, нажав кнопку **«Да»** (См. Рис. 6.6):

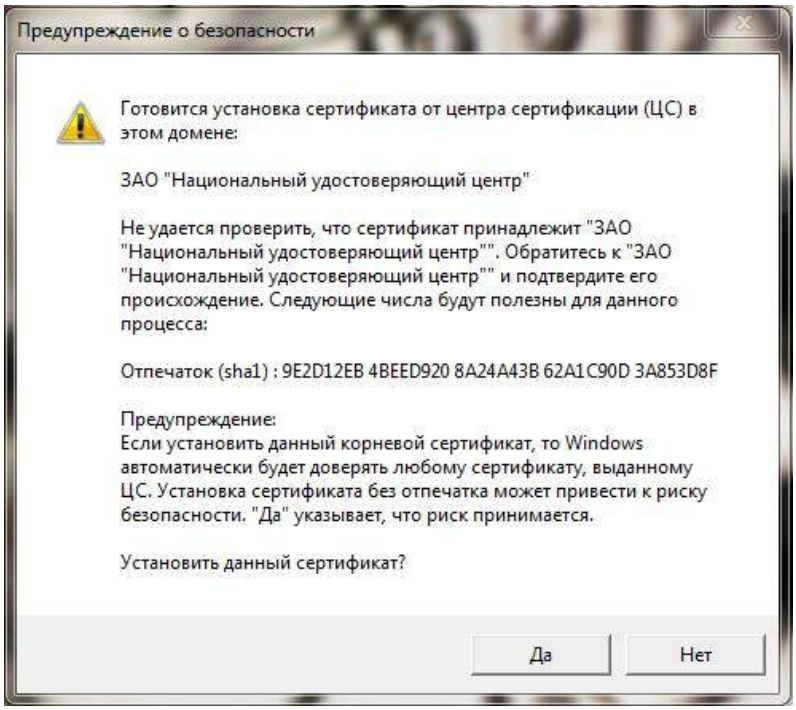

Рис. 6.6. Предупреждение о безопасности

Установка сертификата Удостоверяющего центра **ncarf-v00.cer** или **ncarf-v01.cer** завершена.

7. Установка списка отозванных сертификатов (CRL)

Для начала работы необходимо скачать списки отозванных сертификатов Удостоверяющего Центра. Если сертификат владельца выпущен в период с 05.07.2012 по 26.06.2014, то необходимо скачать сертификат **ncarf-v00.crl.** Если сертификат владельца выпущен в период с 26.06.2014, то необходимо скачать сертификат **ncarf-v01.crl**.

ВНИМАНИЕ! Запомните место, куда Вы сохранили файлы!

Для установки списков отозванных сертификатов Удостоверяющего центра **ncarf-v00.crl** или **ncarf-v01.crl** необходимо открыть в Проводнике папку, куда был сохранен файл **ncarf-v00.crl** или **ncarf-v01.crl** и по нажатию правой кнопки мыши на файле **ncarf-v00.crl** или **ncarf-v01.crl** в контекстном меню выбрать пункт **«Установить список отзыва (CRL)»** (См. Рис. 7.1).

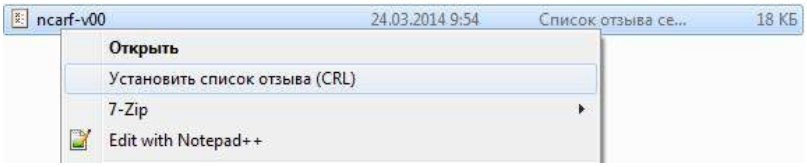

Рис. 7.1. Запуск мастера установки списка отозванных сертификатов

В результате выполненных действий откроется страница приветствия **«Мастера импорта сертификатов»**. В этом окне необходимо нажать кнопку **«Далее»** (См. Рис. 6.2).

Откроется страница **«Хранилище сертификатов»**. На этой странице необходимо установить переключатель в позицию **«Поместить все сертификаты в следующее хранилище»** и затем нажать кнопку **«Обзор»** (См. Рис. 6.3).

Откроется окно**«Выбор хранилища сертификата»**. В этом окне необходимо выбрать хранилище **«Промежуточные центры сертификации»** и нажать кнопку **«ОК»** (См. Рис. 6.4).

Окно **«Выбор хранилища сертификата»** закроется. Мастер установки сертификатов вернется на страницу **«Хранилище сертификатов»**. Необходимо нажать кнопку **«Далее»**. Мастер установки сертификатов перейдет на страницу **«Завершение мастера импорта сертификатов».** Необходимо нажать кнопку **«Готово»** (См. Рис. 6.5).

Установка списка отозванных сертификатов **ncarf-v00.crl** или **ncarf-v01.crl** завершена.

8. Установка личных сертификатов

Для работы с электронной подписью необходимо установить личный сертификат в хранилище **«Личное»** на компьютере пользователя. Установка личного сертификата производится из контейнера закрытого ключа на ключевом носителе.

Для установки личного сертификата из контейнера закрытого ключа на ключевом носителе последовательно выберите меню **Пуск→Настройка→Панель управления** (В случае, если на компьютере установлена ОС – WindowsXP). В появившемся окне выберите **КриптоПро CSP** и запустите ее, дважды кликнув мышкой.

В появившемся окне **«КриптоПРО CSP»** необходимо перейти на вкладку **«Сервис»** и нажать кнопку **«Просмотреть сертификаты в контейнере…»** (См. Рис. 8.1):

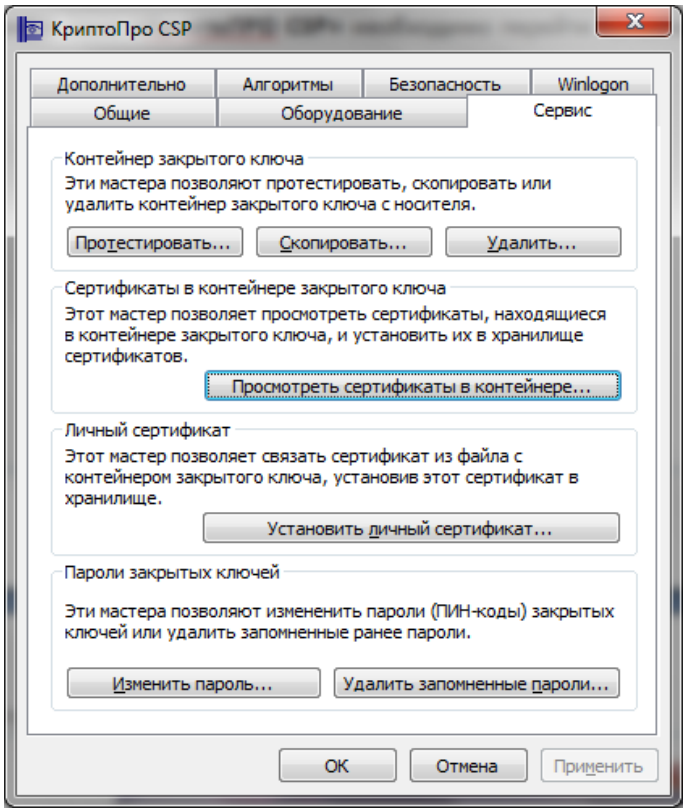

Рис. 8.1. КриптоПРО CSP. Вкладка «Сервис»

В появившемся окне **«Сертификаты в контейнере закрытого ключа»** необходимо нажать кнопку **«Обзор»** (Рис. 8.2):

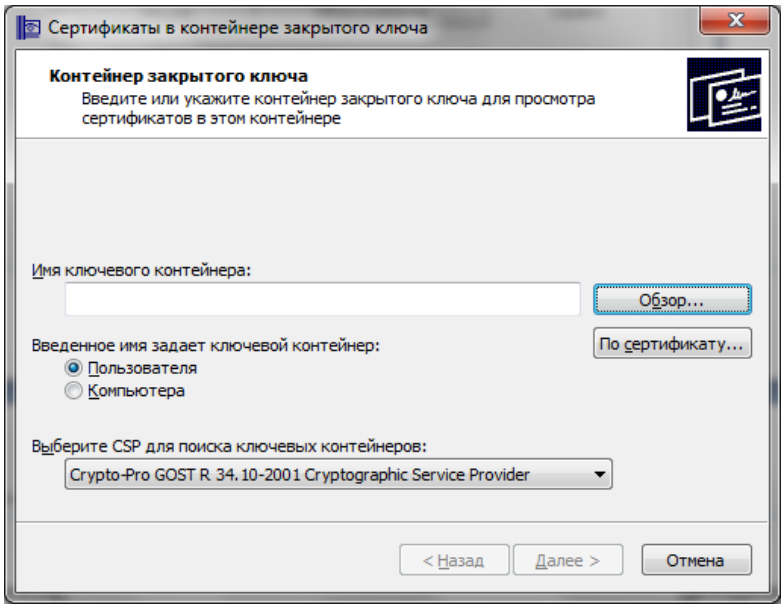

Рис.8.2. Сертификаты в контейнере закрытого ключа

В появившемся окне **«КриптоПРО CSP»** необходимо выбрать требуемый контейнер и нажать кнопку **«ОК»** (Рис. 8.3):

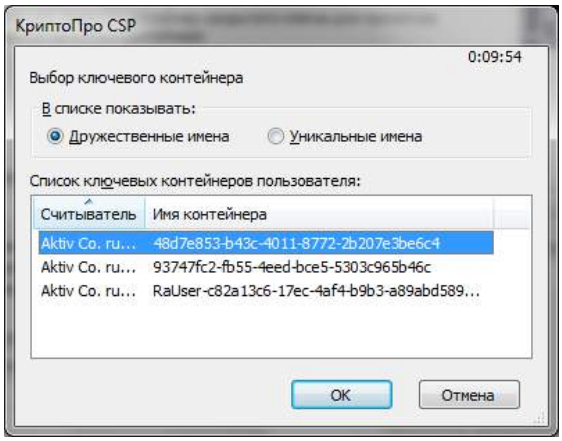

Рис. 8.3. КриптоПРО CSP

Программа вернется в окно **«Сертификаты в контейнере закрытого ключа»**. В поле **«Имя ключевого контейнера»** будет указан контейнер, сертификат из которого будет устанавливаться. Для продолжения необходимо нажать кнопку **«Далее»** (Рис. 8.4):

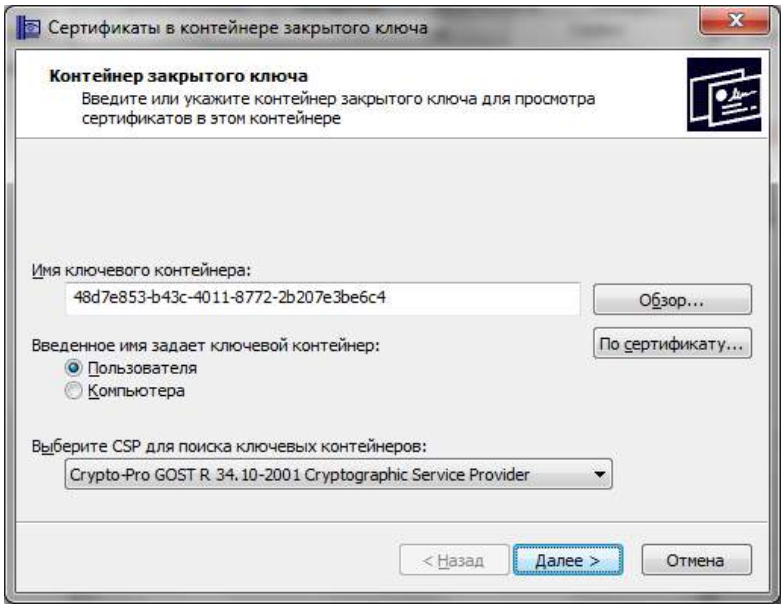

Рис. 8.4. Сертификаты в контейнере закрытого ключа

Отобразится информация об устанавливаемом сертификате. Для установки сертификата пользователя необходимо нажать кнопку **«Установить»** (Рис. 8.5):

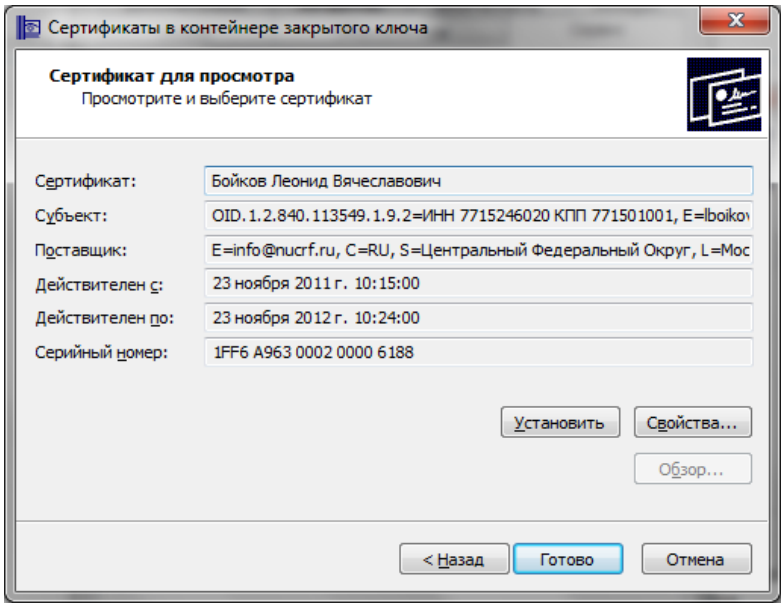

Рис. 8.5. Сертификаты в контейнере закрытого ключа