ESMART®

ESMART Token
Настройка пользовательских приложений

На примере программ:
MS Office 2007
Adobe Acrobat 9
MS Outlook 2007
Mozilla Firefox
Mozilla Thunderbird

Содержание

1. Общая информация

Руководство по предварительной настройке пользовательских приложений предназначено для системных администраторов и опытных пользователей. Для выполнения описанных операций могут потребоваться права администратора.

В данном руководстве описана процедура использования ЭЦП и шифрования с использованием сертификата формата X.509 с ключевой парой, записанной на смарт-карту или USB-ключ.

Для работы ESMART Token с пользовательскими приложениями требуется установка ESMART PKI Client для выбранной операционной системы.

1.1 Использование ESMART Token с программами Microsoft

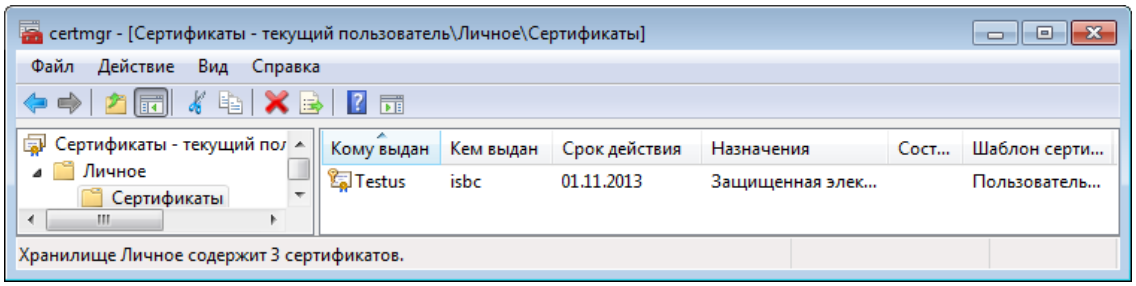
Чтобы программа, например текстовый редактор, могла использовать сертификат для электронной подписи, его копию необходимо поместить в локальное хранилище сертификатов Windows. При этом закрытый ключ со смарт-карты или USB-ключа не извлекается, что обеспечивает высокую степень безопасности. Чтобы получить доступ к закрытому ключу пользователь должен будет ввести ПИН-код, который защищен от перебора.

ESMART Token CSP позволяет автоматически зарегистрировать сертификаты со смарт-карты или USB-ключ в хранилище Windows. Как правило, пользователю не требуется совершать никаких дополнительных действий, работая с пакетом MS Office, когда используются карты или USB-ключи ESMART Token.

1.2 Проверка работоспособности

Процедура может потребоваться, если приложения Windows не видят сертификатов с карты. Чтобы проверить, успешно ли зарегистрирована карта в хранилище Windows, выполните следующие операции (могут потребоваться права администратора):

1. *В командной строке (win+R) наберите certmgr.msc;*
2. *В консоли слева выберите **Сертификаты – текущий пользователь › Личное***



3. *При необходимости, если сертификат не появился сразу, нажмите F5 или кнопку обновить в меню;*
4. *Проверьте в хранилище Доверенные корневые сертификаты наличие соответствующего корневого сертификата;*
5. *Подпишите тестовый документ, например, в редакторе Word или сообщение электронной почты.*

***Внимание!** Приложение ESMART PKI Client позволяет автоматически удалять копию сертификата из локального хранилища Windows при извлечении карты или USB-ключа ESMART Token. Когда карта или USB-ключ будут подключены снова, сертификат автоматически появится в хранилище и будет до-*

ступен для ОС Windows и пользовательских программ. Подробная информация представлена в руководстве администратора ESMART PKI Client.

2. PDF (на примере Adobe Acrobat 9)

2.1 Установка модуля защиты ESMART Token в Adobe Acrobat

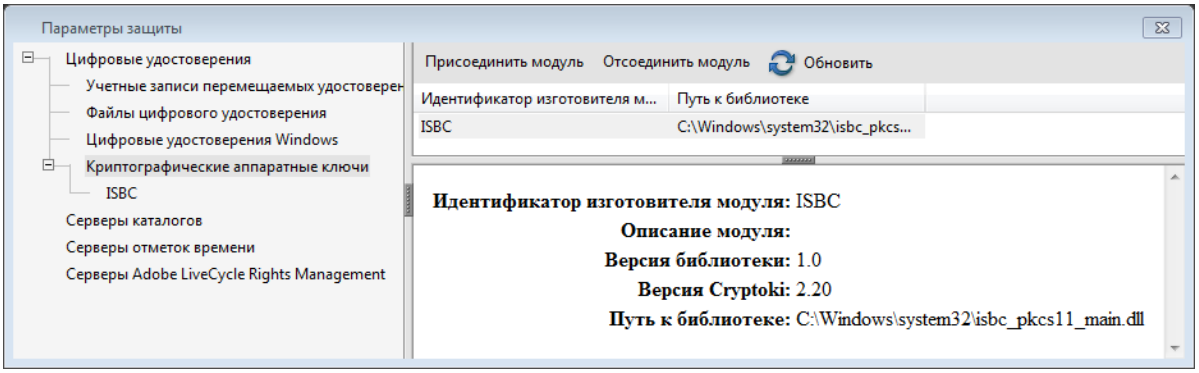
В приложениях Adobe Acrobat 9 и выше есть возможность импортировать модуль PKCS#11 для работы с сертификатами на смарт-картах.

Для установки модуля выберите меню: ***Дополнительно › Параметры защиты.***

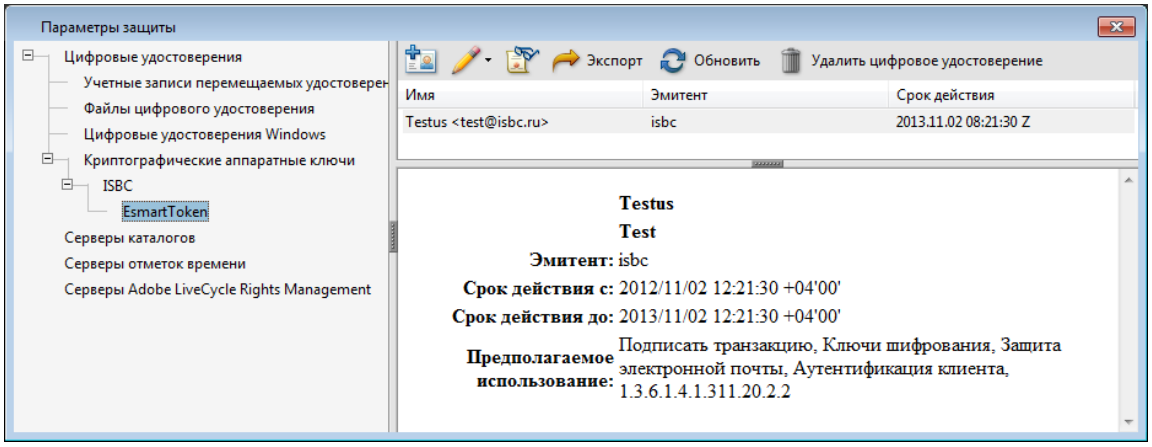
В открывшемся окне откройте в левой панели: ***Цифровые удостоверения › Криптографические аппаратные ключи****.*

В панели справа нажмите ***Присоединить модуль****. В появившемся окне нажмите* ***Обзор*** *и перейдите к файлу* ***isbc_pkcs11_main.dll*** *в папке* ***C:\Windows\System32*** *и нажмите* ***Открыть****.*

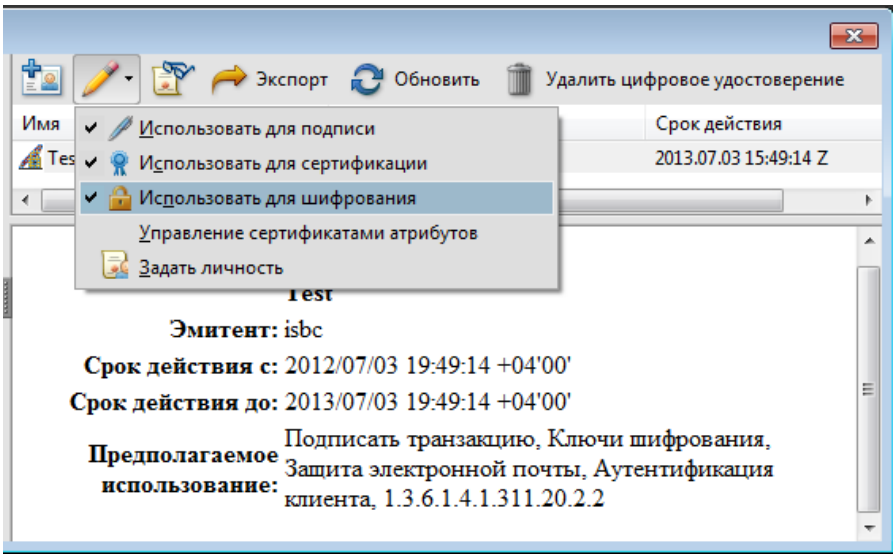
Установленный модуль появится в списке.



В левой панели разверните список под подключенным модулем.
Выберите профиль карты.



Можно просмотреть существующие на карте сертификаты, выбрать их назначение по умолчанию, например, использовать один сертификат для подписи,
а другой для шифрования.

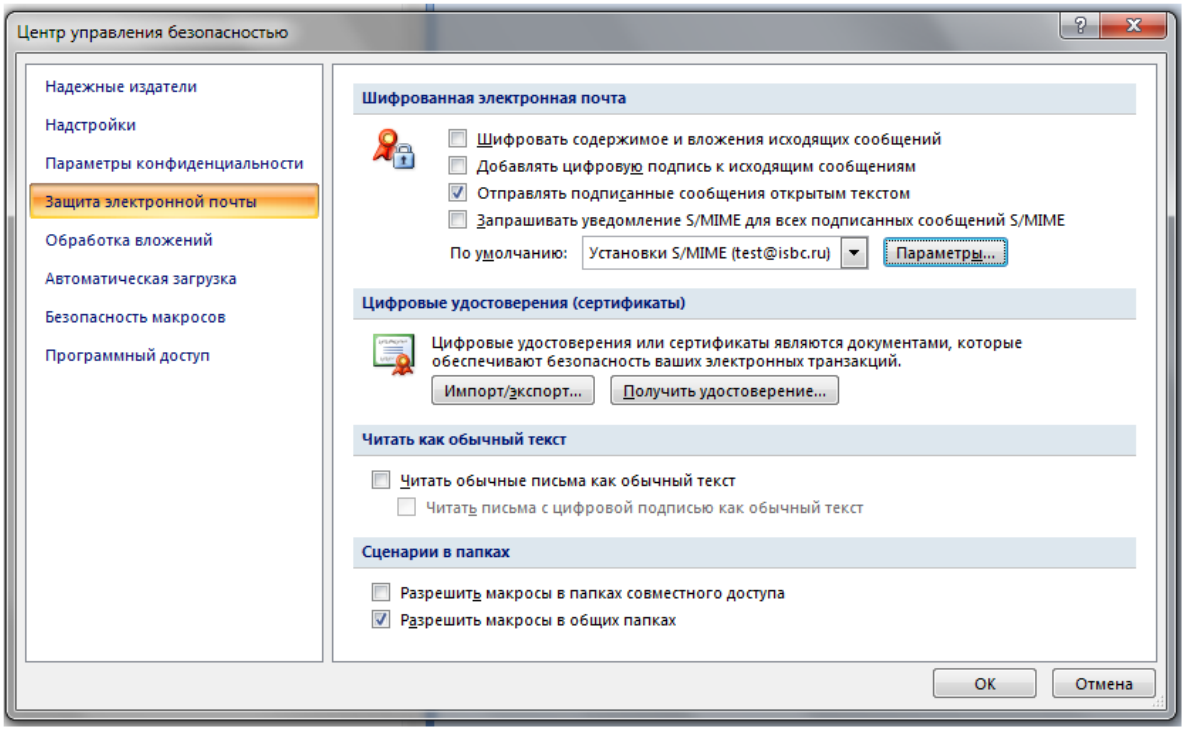


Подпишите или зашифруйте тестовый документ PDF.

3. Почтовый клиент Microsoft OUTLOOK 2007

3.1 Настройка сертификатов

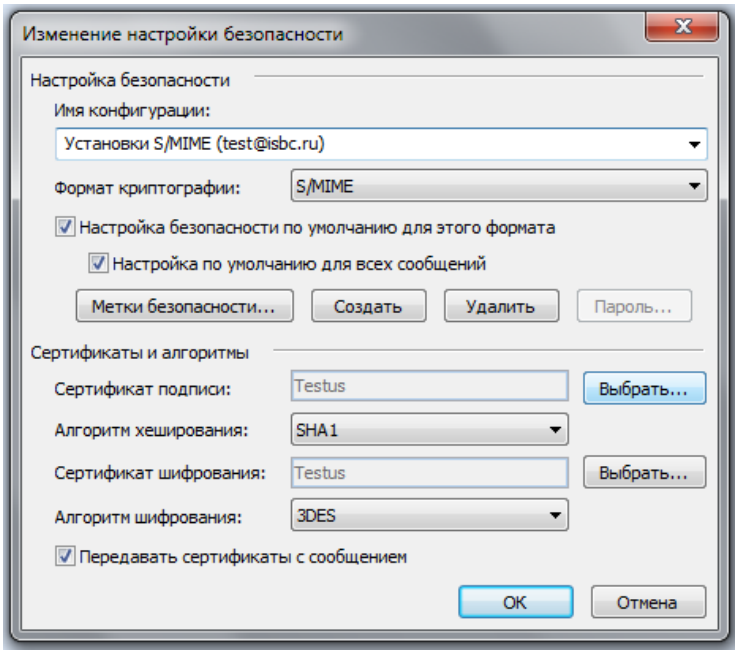
*Выберите в меню **Сервис › Центр управления безопасностью › Защита электронной почты**:*



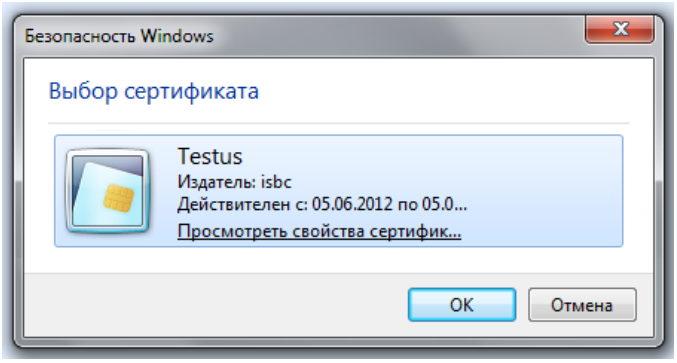
*Установите соответствующие галочки в разделе **Шифрованная электронная почта**, если хотите шифровать сообщения и использовать цифровую подпись по умолчанию для всех писем.*

Устанавливать шифрование и добавлять цифровую подпись можно для каждого индивидуального сообщения. В данной вкладке задаются настройки, которые будут применяться по умолчанию.

*Для выбора сертификата, который будет использоваться для ЭЦП и шифрования, необходимо создать конфигурацию. Как правило, конфигурация создается автоматически. Если этого не произошло, нажмите **Параметры**.*



*В разделе **Сертификаты и алгоритмы** должны быть выбраны сертификаты, которые будут использоваться для подписи и шифрования. Нажмите **Выбрать** и укажите в появившемся окне нужный сертификат:*



При необходимости измените используемые алгоритмы хэширования и шифрования.

Предварительные настройки для использования шифрования и ЭЦП завершены.

4. Почтовый клиент Mozilla Thunderbird

Настройка Mozilla Thunderbird в Windows, Linux и MacOS X осуществляется одинаково. Отличаются только путь и названия динамических библиотек.

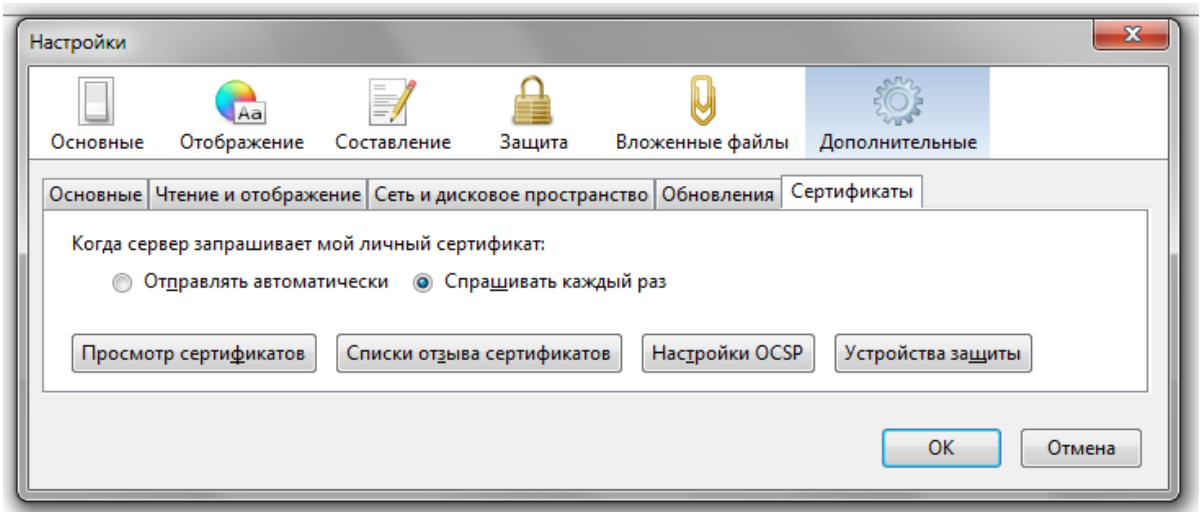
4.1 Настройка сертификатов

Для использования ЭЦП и шифрования электронных сообщений в Thunderbird требуются следующие операции:

- *Установка программного обеспечения ESMART PKI Client при помощи программы-инсталлятора или вручную;*
- *Выбор устройства защиты PKCS#11;*
- *Выбор степени доверия центру сертификации;*
- *Настройка параметров учетной записи.*

*Все операции выполняются из меню **Настройки › Дополнительные › Сертификаты***

4.2 Выбор устройства защиты



*Выберите **Устройства защиты** и нажмите **Загрузить**.*

*В появившемся окне нажмите **Обзор** и перейдите к файлу[1]:*

Windows

C:\Windows\System32\isbc_pkcs11_main.dll

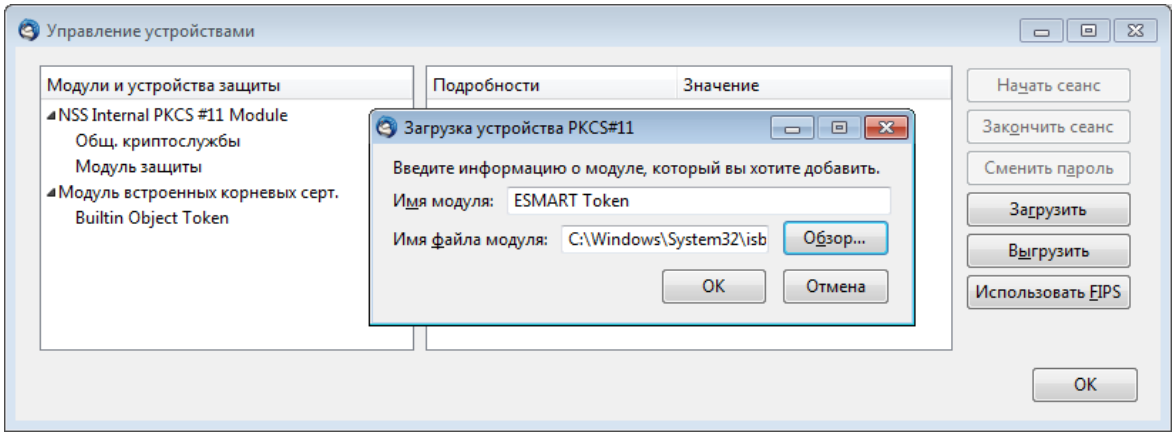
Linux

/usr/lib/ libisbc_pkcs11_main.so

MacOS X

[1] *Путь по умолчанию. Расположение файлов может отличаться, если была выполнена установка вручную, а не при помощи программы-инсталлятора.*

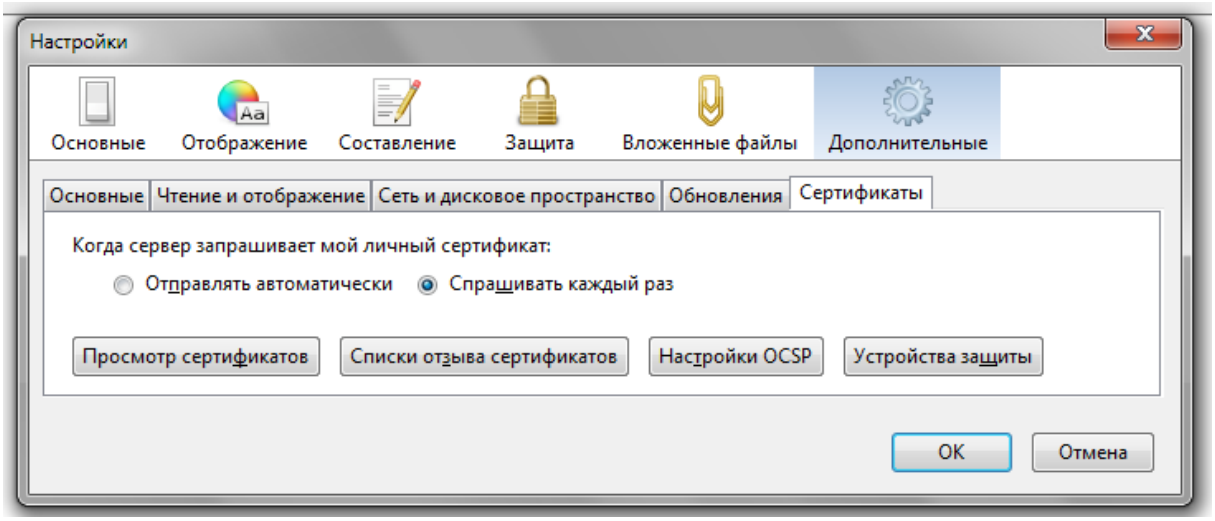
/Applications/ESMART PKI Client/libisbc_pkcs11_main.dylib



Если при добавлении модуля появляется сообщение об ошибке «Невозможно подключить модуль», перезапустите Thunderbird и повторите процедуру.

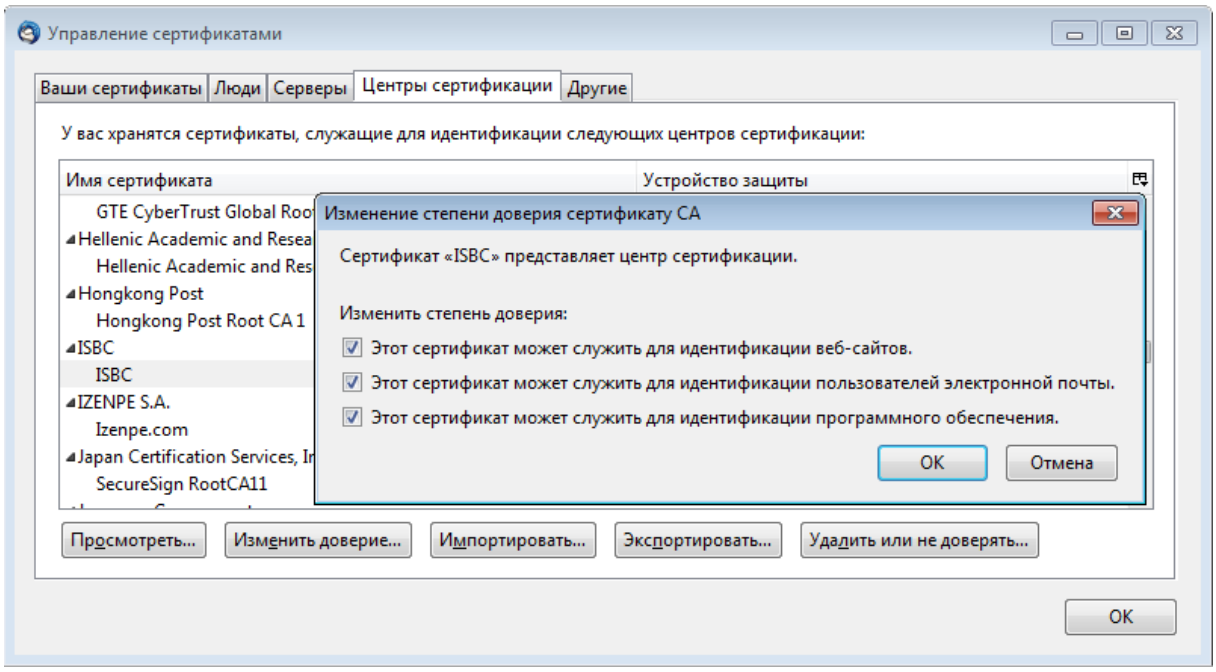
4.3 Выбор степени доверия центру сертификации

Если сертификат выдан корпоративным центром сертификации, необходимо указать степень доверия к CA вручную. Вернитесь на вкладку ***Сертификаты*** *в настройках Thunderbird. Выберите* ***Просмотр сертификатов.***



Во вкладке ***Центры сертификации*** *найдите установленный центр сертификации (в нашем примере ISBC) и измените степень доверия.*

Для подписи и шифровании электронной почты выберите ***Этот сертификат может служить для идентификации пользователей электронной почты****. Остальные опции отметьте при необходимости.*

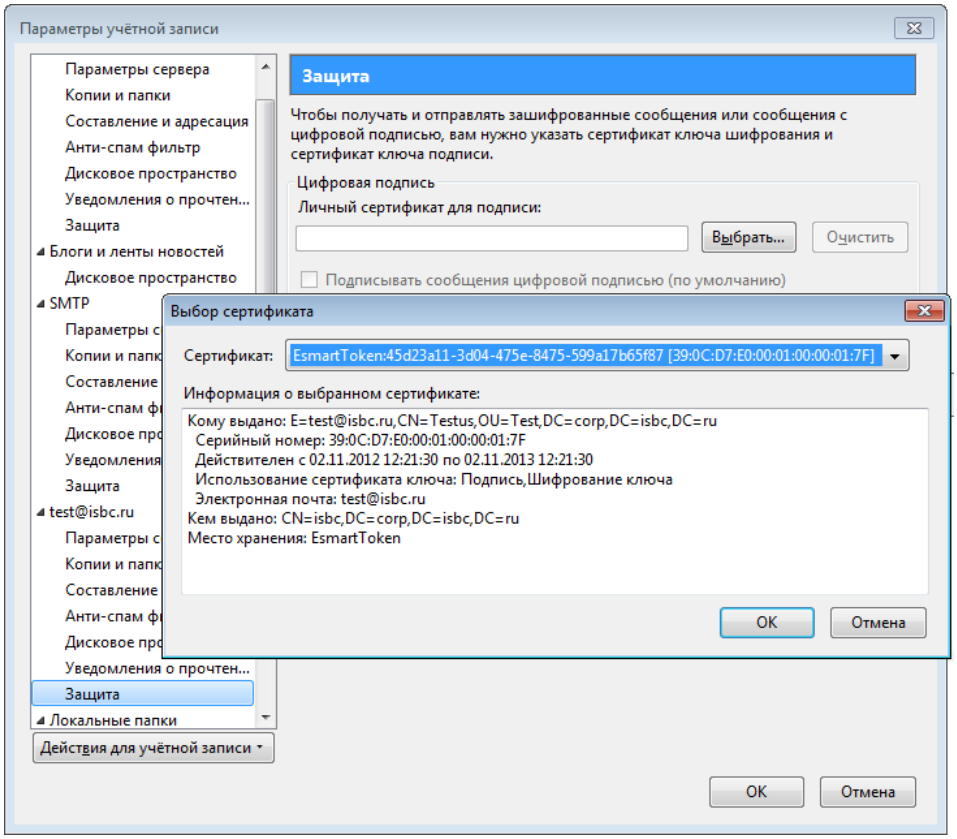


1.1 Настройка параметров учетной записи

Для каждой учетной записи можно настроить индивидуальные параметры защиты и выбрать определенный сертификат (если их несколько). Это расширяет возможности применения ЭЦП и шифрования.

Например, добавление ЭЦП можно назначить по умолчанию для учетной записи корпоративной почты, но не применять защиту к учетной записи для личной почты.

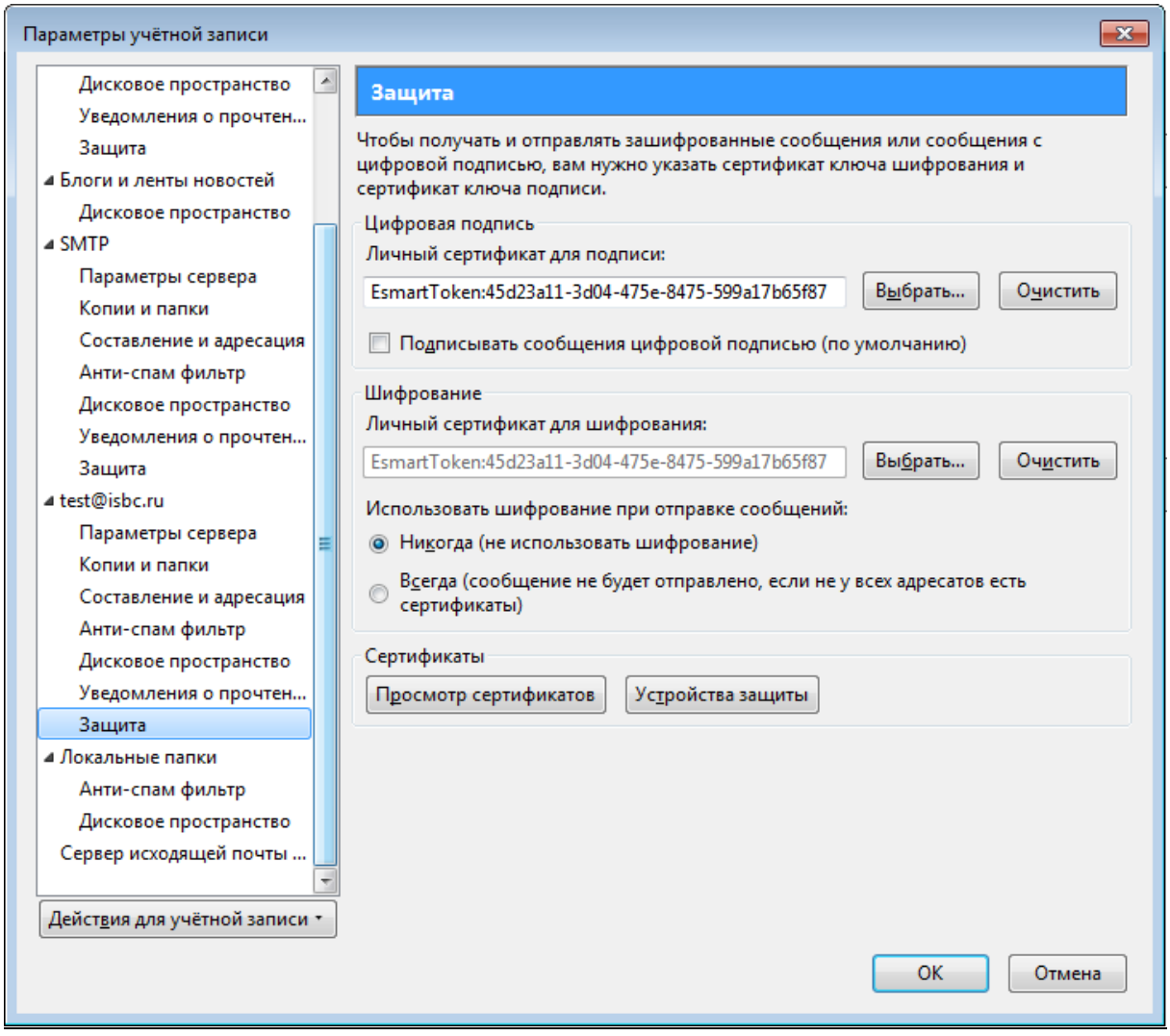
*Откройте **Инструменты › Параметры учетной записи › Защита**:*



Выберите сертификаты, которые будут использоваться, а также отметьте (по желанию) опции ***Подписывать сообщения цифровой подписью (по умолчанию)*** *и* ***Использовать шифрование при отправке сообщений****.*

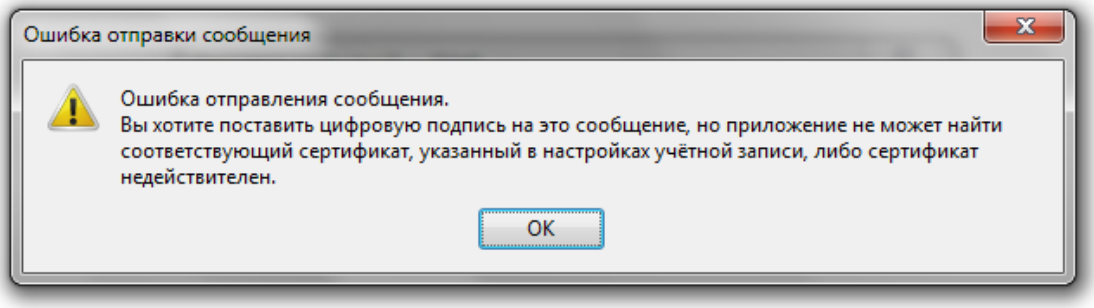
Ставить цифровую подпись и применять шифрование можно к каждому письму индивидуально. В данном окне задаются только значения по умолчанию.

Нажмите ***Выбрать*** *и укажите нужный сертификат (может быть доступно несколько сертификатов).*

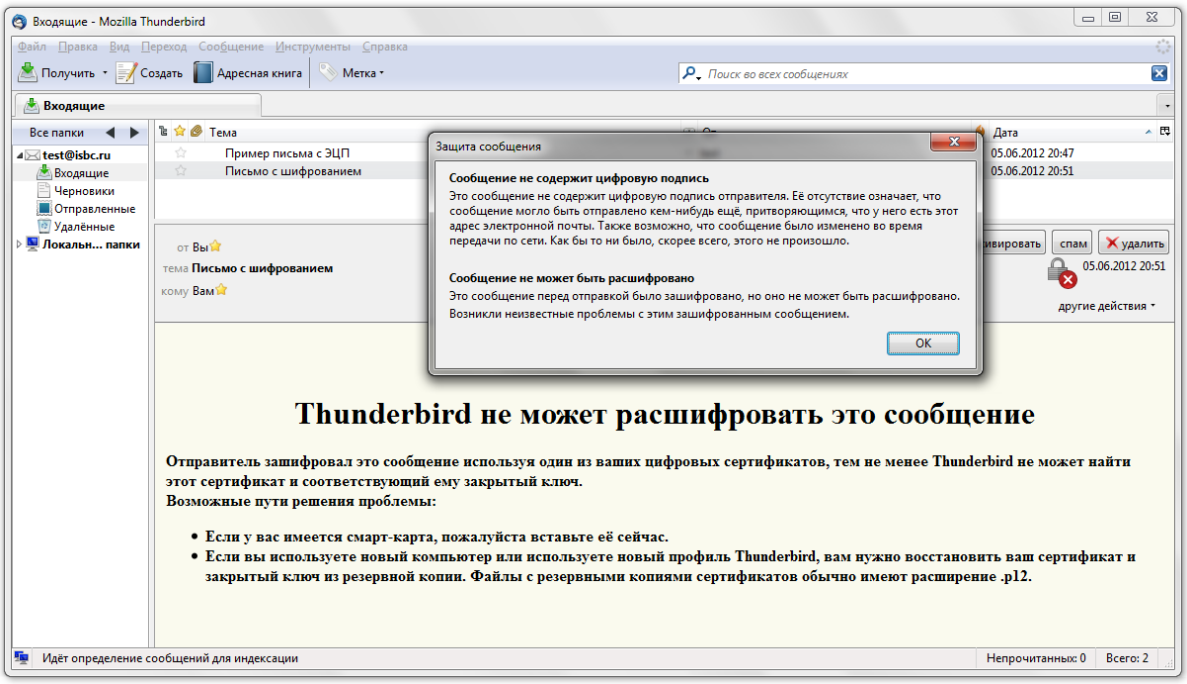


Настройки сертификатов завершены.

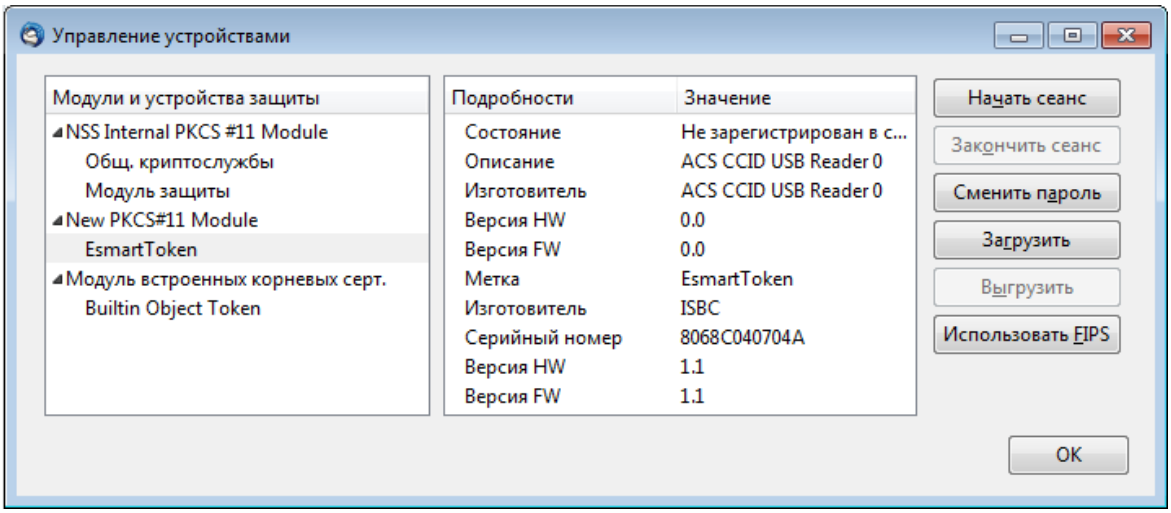
4.4 Возможные проблемы



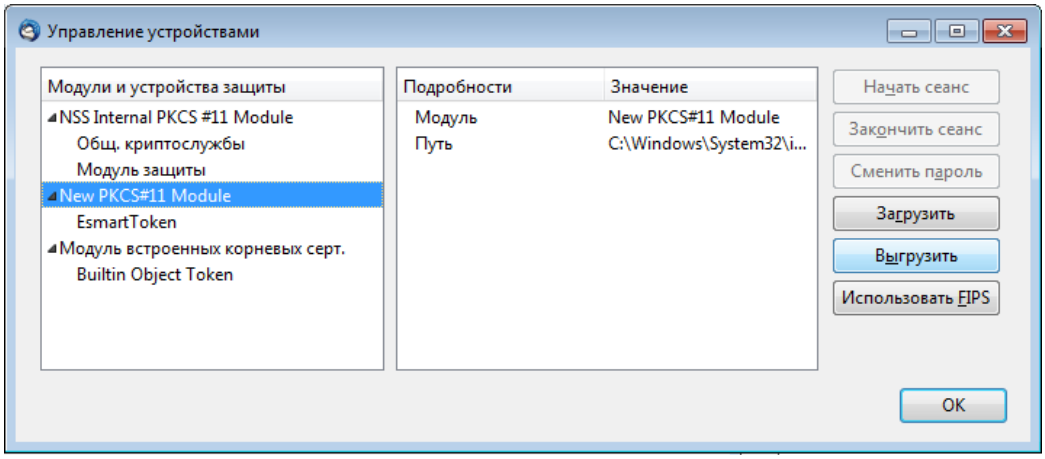
или



В некоторых случаях, например, при использовании нескольких разных USB-ключей или разных считывателей модуль защиты может не подключиться автоматически. Его необходимо запустить повторно.



Если служба отображается, но работает некорректно, необходимо выгрузить службу (подтвердив удаление модуля защиты).



***Обязательно** перезапустите Thunderbird. Без перезапуска программа не сможет загрузить модуль.*

Повторите процедуры добавления модуля PKCS#11 и запуска сеанса, см. стр. 8, а также проверьте параметры использования сертификатов для учетной записи Thunderbird см. стр. 10.

5. Браузер Mozilla Firefox

Настройка Mozilla Firefox в ОС Windows, Linux и MacOS X осуществляется одинаково. Отличаются только путь и названия динамических библиотек.

Для использования ЭЦП и шифрования электронных сообщений в Firefox требуются следующие операции:

- *Установка пакета ESMART PKI Client при помощи программы-инсталлятора или вручную;*
- *Выбор устройства защиты PKCS#11;*
- *Выбор степени доверия центру сертификации.*

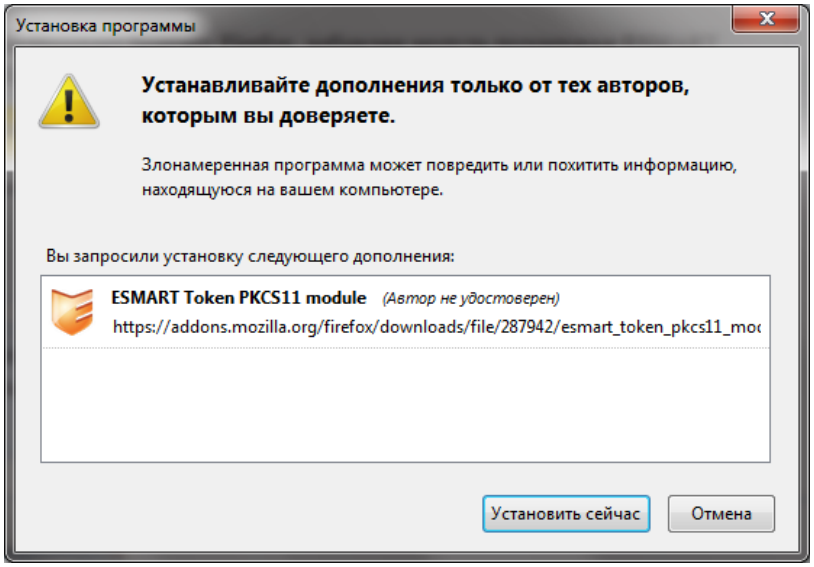
5.1 Автоматическая настройка модуля

После запуска программы-инсталлятора ESMART PKI Client в браузере Firefox автоматически откроется страница установки дополнения ESMART Token PKCS11 module по адресу:

https://addons.mozilla.org/en-US/firefox/addon/esmart-token-pkcs11-module/

Нажмите кнопку добавления модуля "Add to Firefox".

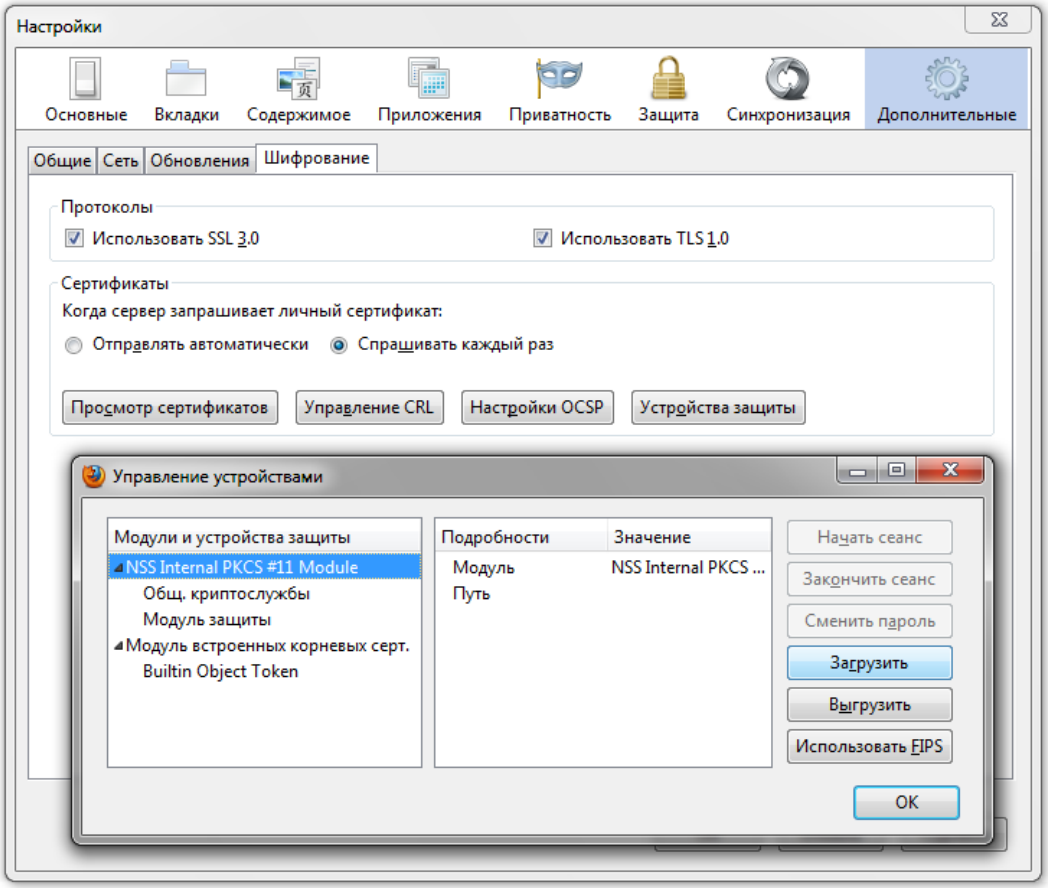
*Подтвердите установку модуля, нажав кнопку «**Установить сейчас**».*



В правом нижнем углу окна браузера должно появиться сообщение об успешной установке модуля.

5.2 Ручная настройка модуля

Выберите: ***Настройки › Дополнительно › Шифрование › Устройства защиты*** *и нажмите* ***Загрузить****.*



Выберите ***Устройства защиты*** *и нажмите* ***Загрузить****.*

В появившемся окне нажмите ***Обзор*** *и перейдите к файлу*[2]*:*

Windows

C:\Windows\System32\isbc_pkcs11_main.dll

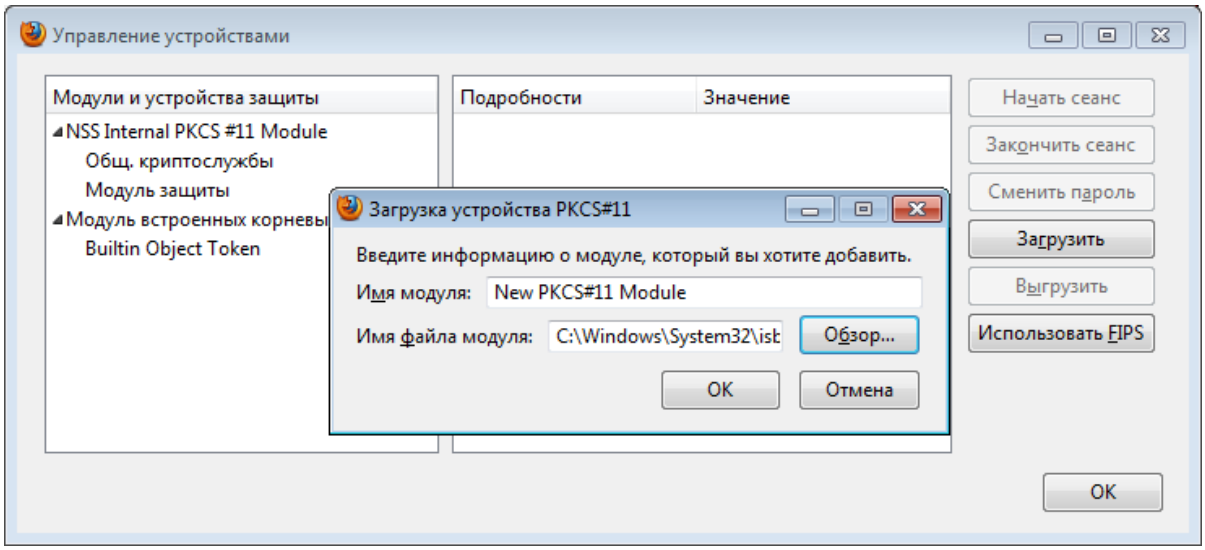
Linux

/usr/lib/ libisbc_pkcs11_main.so

MacOS X

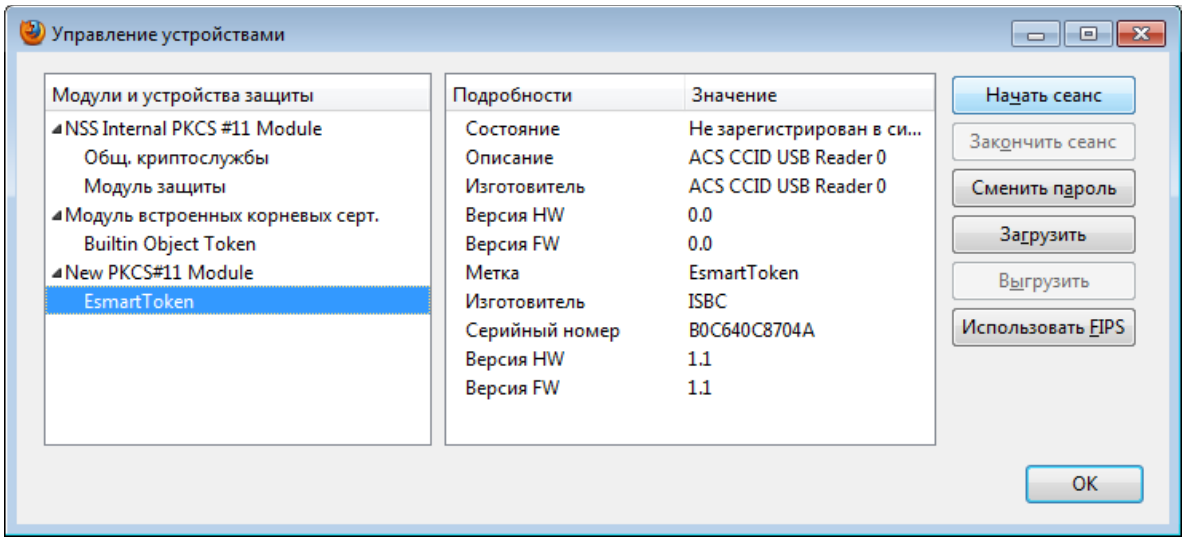
/Applications/ESMART PKI Client/libisbc_pkcs11_main.dylib

[2] *Путь по умолчанию. Расположение файлов может отличаться, если была выполнена установка вручную, а не при помощи программы-инсталлятора.*

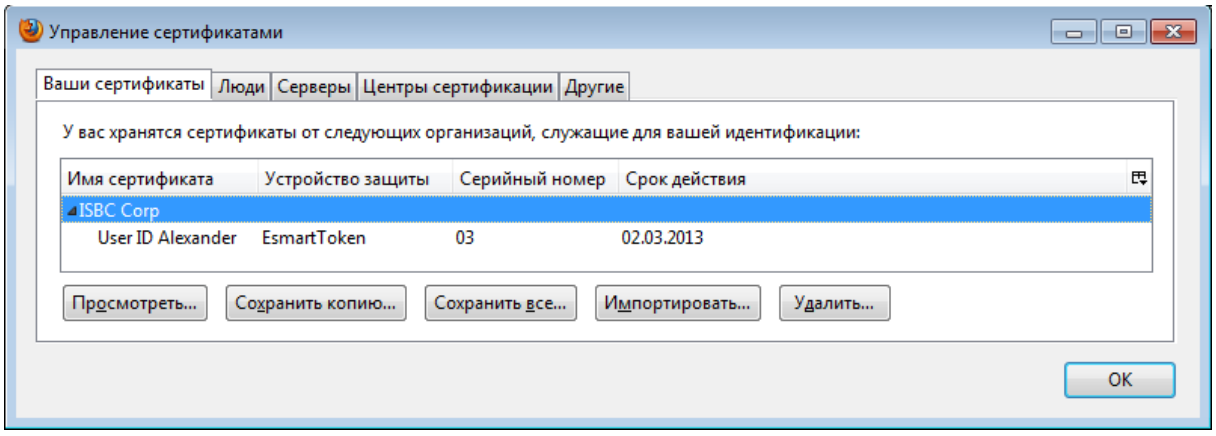


Если при добавлении модуля появляется сообщение об ошибке «Невозможно подключить модуль», перезапустите Firefox и повторите процедуру.

Когда модуль добавлен, появляется информация о карте и считывателе. Для активации модуля нажмите ***Начать сеанс****. Введите ПИН-код карты.*

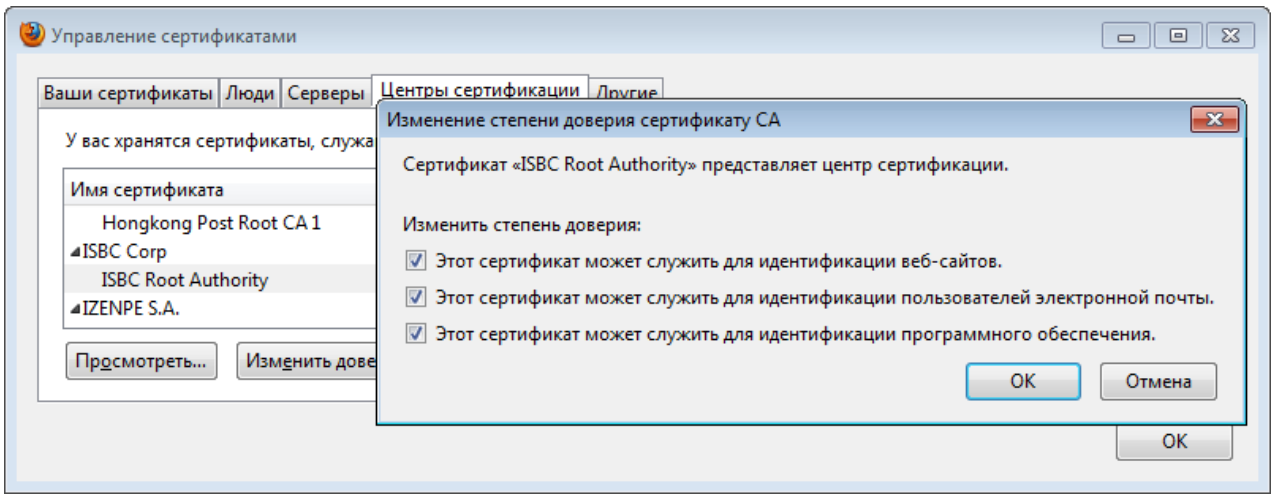


В списке сертификатов должен появиться сертификат с карты:



5.3 Выбор степени доверия центру сертификации

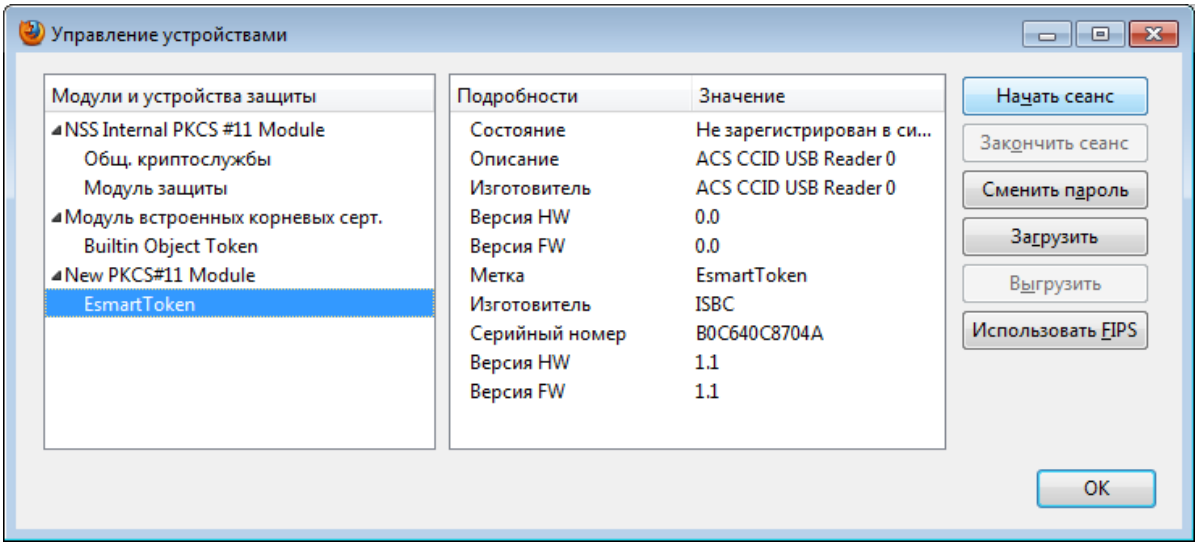
При необходимости измените степень доверия к центру сертификации (настройка автоматически применится и для Thunderbird):



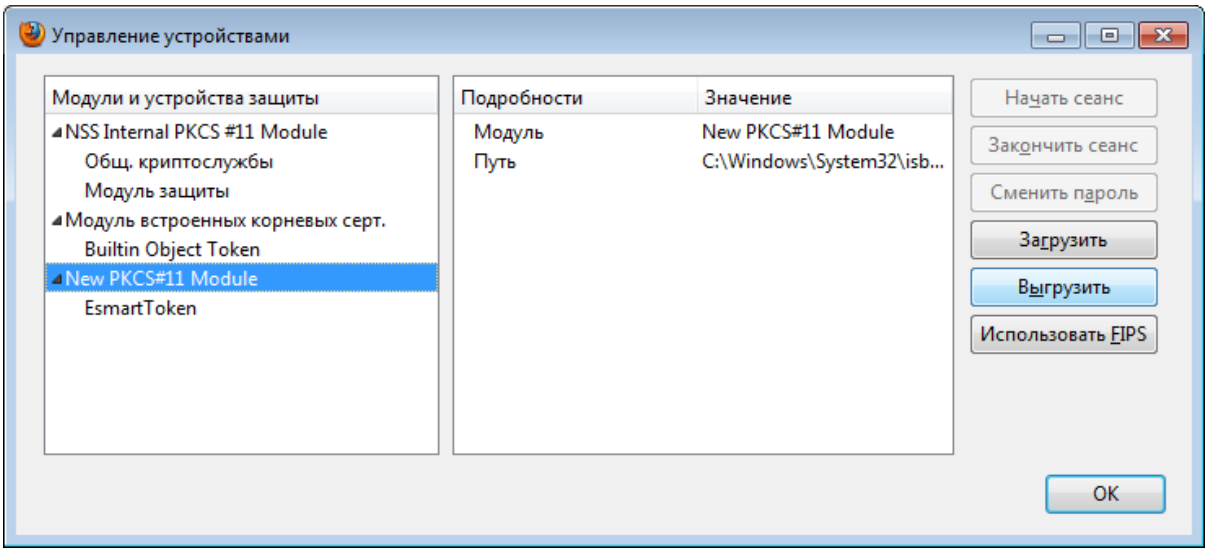
Настройка браузера завершена.

5.4 Возможные проблемы

В некоторых случаях, например, при использовании нескольких токенов или нескольких считывателей модуль защиты может не подключиться автоматически. Его необходимо запустить снова, как описано на стр. 16.



Если служба отображается, но работает не корректно, необходимо выгрузить службу (подтвердив удаление модуля защиты).



Обязательно *перезапустите Firefox. Без перезапуска программа не сможет загрузить модуль повторно. Повторите загрузку модуля.*