

ESMART Token Настройка пользовательских приложений

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



# Содержание

| 1.  | Общая информация                                     | 3 |
|-----|--|---|
| 1.1 | Использование ESMART Token с программами Microsoft   |   |
| 1.2 | Проверка работоспособности                           |   |
| 2.  | PDF (на примере Adobe Acrobat 9)                     | 4 |
| 2.1 | Установка модуля защиты ESMART Token в Adobe Acrobat | 4 |
| 3.  | Почтовый клиент Microsoft OUTLOOK 2007               | 6 |
| 3.1 | Настройка сертификатов                               | 6 |
| 4.  | Почтовый клиент Mozilla Thunderbird                  | 8 |
| 4.1 | Настройка сертификатов                               | 8 |
| 4.2 | Выбор устройства защиты                              | 8 |
| 4.3 | Выбор степени доверия центру сертификации            | 9 |
| 1.1 | Настройка параметров учетной записи                  |   |
| 4.4 | Возможные проблемы                                   |   |
| 5.  | Браузер Mozilla Firefox                              |   |
| 5.1 | Автоматическая настройка модуля                      |   |
| 5.2 | Ручная настройка модуля                              |   |
| 5.3 | Выбор степени доверия центру сертификации            |   |
| 5.4 | Возможные проблемы                                   |   |



## 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

| 🚡 certmgr - [Сертификаты - текущий пользователь\Личное\Сертификаты] |                       |           |               |                 |      |              |  |
|---|-----------------------|-----------|---------------|-----------------|------|--------------|--|
| Файл Действие Вид Справка   |                       |           |               |                 |      |              |  |
| i 🗢 🔿 🖄 🖬 🔏 😫   | ← ⇒   2 🗊   🠇 🖶   🔀 🖬 |           |               |                 |      |              |  |
| 🗊 Сертификаты - текущий пол 🔺                                       | Кому выдан            | Кем выдан | Срок действия | Назначения      | Сост | Шаблон серти |  |
| <ul> <li>Дичное</li> <li>Сертификаты</li> <li>Т</li> </ul>          | 🔄 Testus              | isbc      | 01.11.2013    | Защищенная элек |      | Пользователь |  |
| Хранилище Личное содержит 3 серт                                    | ификатов.             |           |               |                 |      |              |  |

- 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.

| Параметры защиты   | 8                                      |
|--|--|
| <ul> <li>Цифровые удостоверения</li> <li>Учетные записи перемещаемых удостоверен<br/>Файлы цифрового удостоверения</li> <li>Цифровые удостоверения Windows</li> <li>Криптографические аппаратные ключи</li> <li>ISBC</li> <li>Серверы каталогов</li> <li>Серверы отметок времени</li> <li>Серверы Adobe LiveCycle Rights Management</li> </ul> | Присоединить модуль Отсоединить модуль |

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

| Параметры защиты  |   |  |  |   |  |  |
|---|---|--|--|---|--|--|
| Цифровые удостоверения  | 🔖 🥢 - 🔭 🧀 Экспорт                                 | 🛛 🔁 Обновить i Удалить   | цифровое удостоверение                   |   |  |  |
| Учетные записи перемещаемых удостоверен                         | Имя   | Эмитент  | Срок действия                            |   |  |  |
| Фаилы цифрового удостоверения<br>Цифровые удостоверения Windows | Testus <test@isbc.ru></test@isbc.ru>              | isbc   | 2013.11.02 08:21:30 Z                    |   |  |  |
| 🖃 Криптографические аппаратные ключи                            |   |  |  | _ |  |  |
| ен ISBC<br>EsmartToken<br>Серверы каталогов                     | Te<br>Te  | stus<br>st   |  | ~ |  |  |
| Серверы отметок времени   | Эмитент: isb                                      | c  |  |   |  |  |
| Серверы Adobe LiveCycle Rights Management                       | Срок действия с: 20                               | 12/11/02 12:21:30 +04'00'  |  |   |  |  |
|   | Срок действия до: 20                              | 13/11/02 12:21:30 +04'00'  |  |   |  |  |
|   | По<br>предполагаемое<br>эле<br>использование: 1.3 | дписать транзакцию, Ключ<br>ектронной почты, Аутентик<br>.6.1.4.1.311.20.2.2 | и шифрования, Защита<br>фикация клиента, |   |  |  |
|   |   |  |  | - |  |  |

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:

| Центр управления безопасностью  | ? ×  |
|---|--|
| Надежные издатели<br>Надстройки<br>Параметры конфиденциальности<br>Защита электронной почты<br>Обработка вложений<br>Автоматическая загрузка<br>Безопасность макросов<br>Программный доступ | Шифрованная электронная почта            Шифровать содержимое и вложения исходящих сообщений         Добавлять цифровую подпись к исходящим сообщениям         Добавлять подписанные сообщения открытым текстом         Дапрашивать уведомление S/MIME для всех подписанных сообщений S/MIME         По ущолчанию: Установки S/MIME (test@isbc.ru)             Цифровые удостоверения (сертификаты)         Цифровые удостоверения или сертификаты являются документами, которые         обеспечивают безопасность ваших электронных транзакций.         Импорт/экспорт         Долучить удостоверение         Читать как обычный текст         Читать обычные письма как обычный текст         Читать письма с цифровой подписью как обычный текст         Читать письма с цифровой подписью как обычный текст         Читать макросы в папках совместного доступа         Разрешить макросы в общих папках |
|   | ОК Отмена  |

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**.

| Изменение настройки безопасности    |                                |         |  |  |  |  |
|-------------------------------------|--------------------------------|---------|--|--|--|--|
| Настройка безопасности              |                                |         |  |  |  |  |
| Имя конфигурации:                   | Имя конфигурации:              |         |  |  |  |  |
| Установки S/MIME (test@ist          | oc.ru)                         | -       |  |  |  |  |
| Формат криптографии:                | S/MIME                         | -       |  |  |  |  |
| 📝 Настройка безопасности            | по умолчанию для этого формата |         |  |  |  |  |
| 🔽 Настройка по умолча               | нию для всех сообщений         |         |  |  |  |  |
| Метки безопасности                  | Создать Удалить                | Пароль  |  |  |  |  |
| Сертификаты и алгоритмы –           |                                |         |  |  |  |  |
| Сертификат подписи:                 | Testus                         | Выбрать |  |  |  |  |
| Алгоритм хеширования:               | SHA1 🔻                         |         |  |  |  |  |
| Сертификат шифрования:              | Testus                         | Выбрать |  |  |  |  |
| Алгоритм шифрования:                | 3DES 👻                         |         |  |  |  |  |
| Передавать сертификаты с сообщением |                                |         |  |  |  |  |
|                                     | ОК                             | Отмена  |  |  |  |  |

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

Hacmpoйка 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

| ſ | Настройки  |                  |                  |               |                            |                          | ×      |
|---|--|------------------|------------------|---------------|----------------------------|--------------------------|--------|
|   |  |                  |                  |               | Q                          | ,<br>Č                   |        |
| l | Основные   | Отображение      | Составление      | Защита        | Вложенные файлы            | Дополнительные           |        |
|   | Основные   | Ітение и отображ | ение Сеть и диск | овое простра  | анство Обновления С        | ертификаты               |        |
|   | Когда сервер запрашивает мой личный сертификат:<br>Отправлять автоматически  Опрашивать каждый раз |                  |                  |               |                            |                          |        |
|   | Просмот  | р сертификатов   | Списки отзыва    | а сертификато | ов Нас <u>т</u> ройки OCSP | Устройства за <u>щ</u> и | ІТЫ    |
|   |  |                  |                  |               |                            | ОК                       | Отмена |

#### Выберите Устройства защиты и нажмите Загрузить.

В появившемся окне нажмите **Обзор** и перейдите к файлу<sup>1</sup>:

#### Windows

C:\Windows\System32\isbc\_pkcs11\_main.dll

#### Linux

/usr/lib/ libisbc\_pkcs11\_main.so

#### MacOS X

<sup>&</sup>lt;sup>1</sup> 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

| 9 | Управление устройствами  |  |   |
|---|--|--|---|
|   | Модули и устройства защиты<br>a NSS Internal PKCS #11 Module<br>Общ. криптослужбы<br>Модуль защиты<br>a Модуль встроенных корневых серт.<br>Builtin Object Token | Подробности Значение<br>Загрузка устройства РКСЅ#11 ■ ■ ■ ■<br>Введите информацию о модуле, который вы хотите добавить.<br>Имя модуля: ESMART Token<br>Имя файла модуля: C:\Windows\System32\isb О <u>б</u> зор<br>ОК Отмена | На <u>ч</u> ать сеанс<br>Зак <u>о</u> нчить сеанс<br>Сменить п <u>а</u> роль<br>За <u>г</u> рузить<br>В <u>ы</u> грузить<br>Использовать <u>F</u> IPS |
|   |  | ,  | ОК  |

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 СА вручную. Вернитесь на вкладку **Сертификаты** в настройках Thunderbird. Выберите **Просмотр сертификатов.** 

| Настр | ойки   |                          |                        |               |                         |                          | <b>X</b> |
|-------|--|--------------------------|------------------------|---------------|-------------------------|--------------------------|----------|
|       |  |                          |                        |               | U                       | ĘŎŦ                      |          |
| Осн   | овные  | Отображение              | Составление            | Защита        | Вложенные файлы         | Дополнительные           |          |
| Осн   | овные  | Чтение и отображ         | ение Сеть и диск       | овое простра  | нство Обновления С      | ертификаты               |          |
| к     | Когда сервер запрашивает мой личный сертификат:<br>Отправлять автоматически  Спращивать каждый раз |                          |                        |               |                         |                          |          |
|       | Тросмот  | тр серти <u>ф</u> икатов | Списки от <u>з</u> ыва | а сертификато | нас <u>т</u> ройки OCSP | Устройства за <u>ш</u> и | иты      |
|       |  |                          |                        |               |                         | ОК                       | Отмена   |

Во вкладке **Центры сертификации** найдите установленный центр сертификации (в нашем примере <u>ISBC</u>) 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.

| ши сертификаты   Люди   Серв<br>У вас хранятся сертификаты, с  | еры Центры сертификации Другие<br>лужащие для идентификации следующих центров сертификации:   |  |  |  |  |
|--|---|--|--|--|--|
| имя сертификата  | Устроиство защиты   |  |  |  |  |
| <ul> <li>Hellenic Academic and Resea</li> <li>Hellenic Academic and Resea</li> </ul>   | изменение степени доверия сертификату СА<br>Сертификат «ISBC» представляет центр сертификации.  |  |  |  |  |
| ▲Hongkong Post<br>Hongkong Post Root CA 1<br>▲ISBC   | Изменить степень доверия:<br>Этот сертификат может служить для идентификации веб-сайтов.  |  |  |  |  |
| ISBC<br>IZENPE S.A.<br>Izenpe.com  | <ul> <li>Этот сертификат может служить для идентификации пользователей электронной почты.</li> <li>Этот сертификат может служить для идентификации программного обеспечения.</li> </ul> |  |  |  |  |
| <ul> <li>Japan Certification Services, In<br/>SecureSign RootCA11</li> </ul>   | ОК Отмена   |  |  |  |  |
| Пр <u>о</u> смотреть Изм <u>е</u> нить доверие И <u>м</u> портировать Экс <u>п</u> ортировать Уда <u>л</u> ить или не доверять |   |  |  |  |  |

#### 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:

| Параметры учётной записи   | ß   |
|--|---|
| Параметры сервера<br>Копии и папки   | Защита  |
| Составление и адресация<br>Анти-спам фильтр<br>Дисковое пространство                               | цифровой подписью, вам нужно указать сертификат ключа шифрования и<br>сертификат ключа подписи.   |
| Уведомления о прочтен<br>Защита  | Цифровая подпись<br>Личный сертификат для подписи:  |
| <ul> <li>4 Блоги и ленты новостей</li> <li>Лисковое пространство</li> </ul>                        | Выбрать Очистить  |
| ▲ SMTP Выбор сертис  | риката  |
| Копии и папк Сертификат  | EsmartToken:45d23a11-3d04-475e-8475-599a17b65f87 [39:0C:D7:E0:00:01:00:00:01:7F]  |
| Составление Информаци<br>Анти-спам фи  | ия о выбранном сертификате:   |
| Дисковое про<br>Уведомления Действите<br>Защита Использо<br>Электронн<br>Кем выдани<br>Параметры с | но: == тезt@isbc.ru, смэ Тезt0;,00= Тезt,00=сор,0C=:sbc,0C=ru<br>і номер: 39:0C:D7:E0:00:01:00:00:01:7F<br>лен с 02:11.2012 12:21:30 по 02:11.2013 12:21:30<br>вание сертификата ключа: Подпись,Шифрование ключа<br>ная почта: test@isbc.ru<br>о: CN=isbc,DC=corp,DC=isbc,DC=ru<br>нения: EsmartToken |
| Составление  |   |
| Анти-спам фі<br>Дисковое про   | ОК Отмена   |
| Уведомления о прочтен<br>Защита<br>4 Локальные папки   | -   |
| Действия для учётной записи •  |   |
|  | ОК Отмена   |

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).

| Параметры учётной записи   |  |
|--|--|
| Параметры учётной записи<br>Дисковое пространство<br>Уведомления о прочтен<br>Защита<br>Ф Блоги и ленты новостей<br>Дисковое пространство<br>Ф SMTP<br>Параметры сервера<br>Копии и папки<br>Составление и адресация<br>Анти-спам фильтр<br>Дисковое пространство<br>Уведомления о прочтен<br>Защита<br>Ф test@isbc.ru<br>Параметры сервера<br>Копии и папки | Защита         Чтобы получать и отправлять зашифрованные сообщения или сообщения с цифровой подписью, вам нужно указать сертификат ключа шифрования и сертификат ключа подписи.         Цифровая подпись |
| копии и папки<br>Составление и адресация<br>Анти-спам фильтр<br>Дисковое пространство<br>Уведомления о прочтен   | <ul> <li>В<u>с</u>егда (сообщение не будет отправлено, если не у всех адресатов есть сертификаты)</li> <li>Сертификаты</li> <li>П<u>р</u>осмотр сертификатов</li> <li>Устройства защиты</li> </ul>       |
| Защита   |  |
| <ul> <li>Локальные папки</li> <li>Анти-спам фильтр</li> <li>Дисковое пространство</li> <li>Сервер исходящей почты</li> </ul>   |  |
| Дейст <u>в</u> ия для учётной записи т   |  |
|  | ОК Отмена  |

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.

| Модули и устройства защиты                               | Подробности            | Значение  | На <u>ч</u> ать сеанс     |
|--|------------------------|---|---------------------------|
| ▲NSS Internal PKCS #11 Module<br>Общ. криптослужбы       | Состояние<br>Описание  | Не зарегистрирован в с<br>ACS CCID USB Reader 0 | Закончить сеанс           |
| Модуль защиты  | Изготовитель           | ACS CCID USB Reader 0                           | Сменить п <u>а</u> роль   |
| EsmartToken  | Версия HW<br>Версия FW | 0.0   | За <u>г</u> рузить        |
| Модуль встроенных корневых серт.<br>Builtin Object Token | Метка<br>Изготовитель  | EsmartToken<br>ISBC                             | В <u>ы</u> грузить        |
|  | Серийный номер         | 8068C040704A                                    | Использовать <u>F</u> IPS |
|  | Версия FW              | 1.1   |                           |



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

| Модули и устройства защиты                         | Подробности    | Значение                                    | На <u>ч</u> ать сеанс     |
|--|----------------|---|---------------------------|
| ▲NSS Internal PKCS #11 Module<br>Общ. криптослужбы | Модуль<br>Путь | New PKCS#11 Module<br>C:\Windows\System32\i | Закончить сеанс           |
| Модуль защиты                                      |                |   | Сменить пароль            |
| ▲New PKCS#11 Module                                |                |   |                           |
| EsmartToken  |                |   | За <u>г</u> рузить        |
| Модуль встроенных корневых серт.                   |                |   | В <u>ы</u> грузить        |
| Builtin Object Token                               |                |   |                           |
|  |                |   | Использовать <u>F</u> IPS |
|  |                |   |                           |
|  |                |   |                           |

**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

Hacmpoйка Mozilla Firefox в OC 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 РКСЅ#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/

| <b>Э</b> АС   | ОПОЛНЕНИЯ<br>ширения   темы   подборки   ещё   |
|---------------|--|
| 🕈 » Расширени | NR » ESMART Token PKCS11 module  |
|               | ESMART Token PKCS11 module 1.1.3 семперезатоска<br>автор ISBC Ltd.<br>Дополнение настраивает браузер Firefox, добавляя модуль поддержки ESMART<br>Token PKCS#11. |
|               | + Add to Firefox<br>Это дополнение прошло предварительную проверку Mozilla. Узнайте больше   |

Нажмите кнопку добавления модуля "Add to Firefox".

Подтвердите установку модуля, нажав кнопку «Установить сейчас».

| Установка | программы   | 3 |
|-----------|---|---|
|           | Устанавливайте дополнения только от тех авторов,<br>которым вы доверяете.   |   |
|           | Злонамеренная программа может повредить или похитить информацию,<br>находящуюся на вашем компьютере.                                  |   |
| Вы зап    | росили установку следующего дополнения:   |   |
|           | ESMART Token PKCS11 module (Автор не удостоверен)<br>https://addons.mozilla.org/firefox/downloads/file/287942/esmart_token_pkcs11_moc |   |
|           |   |   |
|           |   |   |
|           | Установить сейчас Отмена  | ] |

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.

| П               |  |   |                     | 60  | Ω  |                           |   | 2   | 3          |
|-----------------|--|---|---------------------|---|--|---------------------------|---|---|------------|
|                 |  | 页   | <u>اس</u>           |   |  | G                         | 2   | 50  | 2          |
| Основные        | Вкладки  | Содержимое  | Приложе             | ния Приватн   | ость Защита                                      | Синхрон                   | изация  | Дополнит  | ельнь      |
| Общие Сеть      | Обновлен   | ия Шифрование   | e                   |   |  |                           |   |   |            |
| Протокол        | ы  |   |                     |   |  |                           |   |   |            |
| 🔽 Испо.         | льзовать SSL   | <u>3</u> .0   |                     | V No  | пользовать TLS                                   | <u>1</u> .0               |   |   |            |
| Сертифии        | аты  |   |                     |   |  |                           |   |   |            |
| Когда сер       | вер запраші  | ивает личный се   | ртификат:           |   |  |                           |   |   |            |
| Отпра<br>Отпра  | авлять автом   | атически 🍥 🕻  | Спра <u>ш</u> иватн | каждый раз  |  |                           |   |   |            |
|                 |  |   |                     |   |  |                           |   |   |            |
|                 |  |   |                     |   |  |                           | _   |   |            |
| Про <u>с</u> мо | тр сертифик  | атов Упра <u>в</u> ле   | ение CRL            | Настройки О   | СSP Устр <u>о</u> йс                             | тва защиты                |   |   |            |
| Про <u>с</u> мо | тр сертифик  | атов Упра <u>в</u> ле   | ение CRL            | Наст <u>р</u> ойки Об                                 | СSP Устр <u>о</u> йс                             | тва защиты                |   |   |            |
| Про <u>с</u> мо | тр сертифик<br>равление уст  | атов Упра <u>в</u> ля<br>пройствами   | ение CRL            | Наст <u>р</u> ойки Об                                 | СSP Устр <u>о</u> йс                             | тва защиты                |   | , o <mark>x</mark>  | <b>_</b> ] |
| Про <u>с</u> мо | тр сертифик<br>равление уст  | атов Упра <u>в</u> ле<br>гройствами   | ение CRL            | Наст <u>р</u> ойки Об                                 | СSP Устр <u>о</u> йс                             | тва защиты                |   | , 🗆 🗙   |            |
| Про <u>с</u> мо | тр сертифик<br>равление уст<br>одули и устро   | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты  | ение CRL            | Настройки ОС  | СSP) Устр <u>о</u> йс<br>Значение                | тва защиты                | Нацат   | р 🔲 🔜 🗙   |            |
|                 | тр сертифик<br>равление уст<br>раули и устри   | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>KCS #11 Module  | ение CRL            | Настройки ОО<br>одробности<br>модуль                  | СSP Устройс<br>Значение<br>NSS Internal          | тва защиты<br>РКСS        | на <u>ч</u> ат<br>Зак <u>о</u> нч   | рани и простории и простори<br>По сеанс |            |
|                 | тр сертифик<br>равление уст<br>одули и устри<br>OS Internal P<br>Общ. крипт  | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>KCS #11 Module<br>гослужбы  | ение CRL            | Настройки ОС<br>одробности<br>Модуль<br>Путь          | СSP Устр <u>о</u> йс<br>Значение<br>NSS Internal | тва защиты<br>РКСS        | На <u>ч</u> ат<br>Зак <u>о</u> нчи  | з сеанс<br>ть сеанс<br>ить сеанс  |            |
| Про <u>с</u> мо | тр сертифик<br>равление уст<br>одули и устри<br>ISS Internal P<br>Общ. крипт<br>Модуль зац<br>logyль встро                 | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>KCS #11 Module<br>гослужбы<br>циты<br>ненных корневых             | ение CRL            | Наст <u>р</u> ойки ОС<br>одробности<br>Модуль<br>Путь | СSP Устр <u>о</u> йс<br>Значение<br>NSS Internal | тва защиты<br>РКСS        | На <u>ч</u> ат<br>Зак <u>о</u> нчи<br>Сменит                                  | р — Х<br>гь сеанс<br>ить сеанс<br>гь п <u>а</u> роль  |            |
| Про <u>с</u> мо | тр сертифик<br>равление уст<br>одули и устри<br>ISS Internal P<br>Общ, крипт<br>Модуль зац<br>loдуль встро<br>Builtin Obje | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>KCS #11 Module<br>гослужбы<br>циты<br>ченных корневых<br>ct Token | ение CRL            | Наст <u>р</u> ойки ОС<br>одробности<br>Модуль<br>Путь | СSP Устр <u>о</u> йс<br>Значение<br>NSS Internal | тва защиты<br>РКСS        | На <u>ч</u> ат<br>Зак <u>о</u> нчи<br>Сменит<br>За <u>г</u> р                 | р — Х<br>ть сеанс<br>ить сеанс<br>гь п <u>а</u> роль<br>рузить  |            |
|                 | тр сертифик<br>равление уст<br>одули и устри<br>ISS Internal P<br>Общ, крипт<br>Модуль заш<br>loдуль встро<br>Builtin Obje | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>КСS #11 Module<br>гослужбы<br>циты<br>ченных корневых<br>ct Token | ение CRL            | Наст <u>р</u> ойки ОС<br>одробности<br>Модуль<br>Путь | СSP Устр <u>о</u> йс<br>Значение<br>NSS Internal | тва защиты<br>РКСS (      | Нацат<br>Закончи<br>Сменит<br>За <u>г</u> р                                   | р П Х<br>ть сеанс<br>ить сеанс<br>гь п <u>а</u> роль<br>рузить  |            |
|                 | тр сертифик<br>равление уст<br>SS Internal P<br>Общ, крипт<br>Модуль зац<br>loдуль встро<br>Builtin Obje                   | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>KCS #11 Module<br>гослужбы<br>циты<br>ченных корневых<br>ct Token | ение CRL            | Наст <u>р</u> ойки ОС<br>одробности<br>Модуль<br>Путь | СSP Устр <u>о</u> йс<br>Значение<br>NSS Internal | тва защиты<br>РКСS (      | на <u>ч</u> ат<br>Зак <u>о</u> нчи<br>Сменит<br>За <u>гр</u><br>В <u>ы</u> гр | ть сеанс<br>ить сеанс<br>ть пароль<br>рузить<br>рузить<br>овать <u>F</u> IPS  |            |
|                 | тр сертифик<br>равление уст<br>одули и устри<br>ISS Internal P<br>Общ. крипт<br>Модуль зац<br>loдуль встро<br>Builtin Obje | атов Упра <u>в</u> ли<br>гройствами<br>ойства защиты<br>КСS #11 Module<br>гослужбы<br>циты<br>ченных корневых<br>ct Token | ение CRL            | Наст <u>р</u> ойки ОС<br>одробности<br>Модуль<br>Путь | СSP Устр <u>о</u> йс<br>Значение<br>NSS Internal | тва защиты<br>РКСS [<br>[ | Нацат<br>Зак <u>о</u> нчи<br>Сменит<br>Загр<br>В <u>ы</u> гр                  | р — Х<br>ть сеанс<br>ить сеанс<br>гь п <u>а</u> роль<br>рузить<br>рузить<br>овать <u>F</u> IPS                              |            |

#### Выберите Устройства защиты и нажмите Загрузить.

В появившемся окне нажмите **Обзор** и перейдите к файлу<sup>2</sup>:

#### 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

**ESMART ESMART Token – Настройка пользовательских приложений** версия 3.1 от 23.01.2015

<sup>&</sup>lt;sup>2</sup> Путь по умолчанию. Расположение файлов может отличаться, если была выполнена

установка вручную, а не при помощи программы-инсталлятора.

| Модули и устройства защиты                         | Подробн                   | ости Значе             | ние                 | На <u>ч</u> ать сеанс     |
|--|---------------------------|------------------------|---------------------|---------------------------|
| ANSS Internal PKCS #11 Module<br>Общ. криптослужбы |                           |                        |                     | Закончить сеанс           |
| Модуль защиты                                      | Загрузка устройств        | a PKCS#11              |                     | Сменить пароль            |
| Builtin Object Token                               | Введите информаци         | ю о модуле, который вь | и хотите добавить.  | За <u>г</u> рузить        |
| 1  | И <u>м</u> я модуля: New  | PKCS#11 Module         |                     | В <u>ы</u> грузить        |
| 1  | Имя <u>ф</u> айла модуля: | C:\Windows\System32    | ∖isb O <u>6</u> 30p | Использовать <u>F</u> IPS |
|  |                           | ОК                     | Отмена              |                           |
|  |                           |                        |                     | ]                         |

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.

| Модули и устройства защиты  | Подробности  | Значение   | На <u>ч</u> ать сеанс  |
|---|--|--|--|
| <ul> <li>ANSS Internal PKCS #11 Module</li> <li>Общ. криптослужбы</li> <li>Модуль защиты</li> <li>Модуль встроенных корневых серт.<br/>Builtin Object Token</li> <li>ANew PKCS#11 Module</li> </ul> | Состояние<br>Описание<br>Изготовитель<br>Версия HW<br>Версия FW<br>Метка | He зарегистрирован в си<br>ACS CCID USB Reader 0<br>ACS CCID USB Reader 0<br>0.0<br>0.0<br>EsmartToken | Зак <u>о</u> нчить сеанс<br>Сменить пароль<br>За <u>г</u> рузить |
| EsmartToken   | Изготовитель<br>Серийный номер<br>Версия HW<br>Версия FW                 | ISBC<br>B0C640C8704A<br>1.1<br>1.1   | Использовать <u>F</u> IPS  |

В списке сертификатов должен появиться сертификат с карты:

| 🥹 Управление сертификат | ами                    |                      |                        |            |    |
|-------------------------|------------------------|----------------------|------------------------|------------|----|
| Ваши сертификаты Люд    | и Серверы Центры се    | ртификации Други     | e                      |            |    |
| У вас хранятся сертифи  | икаты от следующих ори | ганизаций, служащи   | ие для вашей идент     | гификации: |    |
| Имя сертификата         | Устройство защиты      | Серийный номер       | Срок действия          |            | E. |
| ISBC Corp               |                        |                      |                        |            |    |
| User ID Alexander       | EsmartToken            | 03                   | 02.03.2013             |            |    |
| Пр <u>о</u> смотреть    | охранить копию         | охранить <u>в</u> се | 1 <u>м</u> портировать | Удалить    |    |
|                         |                        |                      |                        |            | ОК |



#### 5.3 Выбор степени доверия центру сертификации

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

| 🥹 Управление сертификатами                  |  |
|---|--|
| Ваши сертификаты Люди Серверы               | Центры сертификации Лоугие<br>Изменение степени доверия сертификату СА                     |
| Имя сертификата                             | Сертификат «ISBC Root Authority» представляет центр сертификации.                          |
| Hongkong Post Root CA 1<br>⊿ISBC Corp       | Изменить степень доверия:<br>👽 Этот сертификат может служить для идентификации веб-сайтов. |
| ISBC Root Authority<br>▲IZENPE S.A.         | Этот сертификат может служить для идентификации пользователей электронной почты.           |
| Пр <u>о</u> смотреть Изм <u>е</u> нить дове | ОК Отмена  |
|   | ОК   |

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.

| Модули и устройства защиты   | Подробности  | Значение   | На <u>ч</u> ать сеанс   |
|--|--|--|---|
| <ul> <li>ANSS Internal PKCS #11 Module<br/>Общ, криптослужбы<br/>Модуль защиты</li> <li>Модуль встроенных корневых серт.<br/>Builtin Object Token</li> <li>New PKCS#11 Module<br/>EsmartToken</li> </ul> | Состояние<br>Описание<br>Изготовитель<br>Версия HW<br>Версия FW<br>Метка<br>Изготовитель | He зарегистрирован в си<br>ACS CCID USB Reader 0<br>ACS CCID USB Reader 0<br>0.0<br>0.0<br>EsmartToken<br>ISBC | Зак <u>о</u> нчить сеанс<br>Сменить п <u>а</u> роль<br>За <u>г</u> рузить<br>В <u>ы</u> грузить |
|  | Серийный номер<br>Версия HW<br>Версия FW   | B0C640C8704A<br>1.1<br>1.1   | Использовать <u>F</u> IPS   |

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

| Модули и устройства защиты  | Подробности    | Значение                                      | На <u>ч</u> ать сеанс  |
|---|----------------|---|--|
| <ul> <li>▲ NSS Internal PKCS #11 Module<br/>Общ, криптослужбы<br/>Модуль защиты</li> <li>▲ Модуль встроенных корневых серт.<br/>Builtin Object Token</li> <li>▲ New PKCS#11 Module<br/>EsmartToken</li> </ul> | Модуль<br>Путь | New PKCS#11 Module<br>C:\Windows\System32\isb | Зак <u>о</u> нчить сеанс<br>Сменить п <u>а</u> роль<br>За <u>г</u> рузить<br>В <u>ы</u> грузить<br>Использовать <u>F</u> IPS |

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

