

РУТОКЕН®

Российское средство аутентификации

**Rutoken
для MacOS X**

Решение **Rutoken для Mac OS X** включает драйвер Rutoken для кроссплатформенного проекта **pcsc-lite** и набор утилит из проекта OpenSC. Функционально **Rutoken для Mac OS X** представляет собой полную копию решения **Rutoken для Linux**.

Все программное обеспечение распространяется в виде исходных текстов, что позволяет применить его на любой платформе (PowerPC и Intel). Разработка велась для Mac OS X 10.5.2 на платформе Intel.

Возможности (аналогично **Rutoken для Linux**):

- Авторизация пользователей в сетях и на рабочих станциях
- Вход по предъявлению токена
- Подключение к серверу по предъявлению токена
- Безопасность электронной переписки
- Электронная цифровая подпись почтовых сообщений
- Шифрование почтовых сообщений
- Надежное хранение и безопасное использование сертификатов, паролей и так далее
- Применение Rutoken в качестве защищенного хранилища любой персональной информации о пользователе

Важная информация

Все программное обеспечение Rutoken для операционных систем семейства *nix и Mac OS X работает **исключительно** с идентификаторами аппаратной версии 2.0 и выше (Rutoken S).

Пример установки

Фреймворк **pcsc-lite** уже встроен в Mac OS X версии 10.5 и выше, а набор утилит **OpenSC** доступен в виде универсального инсталлятора формата **dmg** с сайта проекта SCA (Smart Card for Apple) от OpenSC Project.

Соответственно, для работы драйвера необходимо установить библиотеку **libusb** и драйвер Rutoken следующими командами:

Важная информация

Все действия производились на Mac OS X версии 10.5.2. В других версиях ОС пути могут отличаться от указанных.

Установка библиотеки libusb

1. Загрузите исходные тексты библиотеки:

```
# curl http://downloads.sourceforge.net/libusb/libusb-0.1.12.tar.gz -o libusb-0.1.12.tar.gz
```

2. Разархивируйте их:

```
# tar xf libusb-0.1.12.tar.gz
# cd libusb-0.1.12
```

3. Загрузите патч для компиляции под Mac OS X:

```
# curl http://libusb.darwinports.com/dports/devel/libusb/files/patch-darwin.c.diff -o patch-darwin.c.diff
```

4. Примените патч к исходным текстам библиотеки:

```
# patch -p0 < patch-darwin.c.diff
```

5. Сконфигурируйте, соберите и установите в систему:

```
# ./configure --prefix=/Developer/SDKs/MacOSX10.5.sdk/usr --disable-build-docs
# make
```

6. После выполнения следующей команды, возможно, потребуется ввести пароль текущего пользователя (т. е. не пользователя **root**):

```
# sudo make install
```

Библиотека **libusb** установлена и может быть использована драйвером Rutoken.

Установка драйвера Rutoken

Установите драйвер Rutoken (<http://rutoken.ru/hotline/download/nix/>):

```
# tar xf ccid-rutoken.tar.bz2
# cd ccid-rutoken
# MacOSX/configure
# make
# sudo make install
```

Утилиты для работы с Rutoken

Для работы с Rutoken понадобится комплект утилит **OpenSC**, который можно установить, воспользовавшись инсталлятором **SCA (Smart Card for Apple)** от **OpenSC Project** (<http://www.opensc-project.org/sca/>). Комплект распространяется в формате **.dmg** и содержит все необходимые утилиты и библиотеки для работы с Rutoken:

rutoken-tool	Модуль позволяет использовать встроенные в Rutoken возможности симметричной криптографии, хеширования
opensc-explorer	Просмотр и редактирование файловой системы токена
opensc-pkcs11.so	Библиотека, реализующая стандарт PKCS#11. Она используется Firefox и Thunderbird для работы с сертификатами, загруженными на токен

Модули устанавливаются в каталог **/Library/OpenSC** (исполняемые файлы в подкаталог **/Library/OpenSC/bin**, библиотеки – в **/Library/OpenSC/lib**).

Примеры использования

Создание и запись сертификата на Rutoken

1. Создайте сертификаты, которые будут временно храниться в ~/demoCA:

```
# /System/Library/OpenSSL/misc/CA.pl -newca
```

2. Создайте ключи:

```
# openssl x509 -in demoCA/cacert.pem -days 3650 -out demoCA/cacert.pem -  
signkey demoCA/private/cakey.pem  
# /System/Library/OpenSSL/misc/CA.pl -newreq
```

3. Процесс подписывания:

```
# /System/Library/OpenSSL/misc/CA.pl -sign
```

4. Сконвертируйте секретный ключ и сертификат в формат DER:

```
# openssl rsa -in newkey.pem -outform DER -out key.der  
# openssl x509 -in newcert.pem -outform DER -out cert.der
```

5. Отформатируйте Rutoken:

```
# pkcs15-init -E -p rutoken
```

6. Запишите сертификат и секретный ключ на Rutoken:

```
# pkcs11-tool --write-object cert.der --type cert --login --id 1 --label  
"user"  
# pkcs11-tool --write-object key.der --type privkey --login --id 1 --label  
"user"
```

Важная информация

Из-за различий в реализации библиотеки **pkcs11** в ***nix** и **MS Windows** сертификаты, экспортированные в память токена под ОС Windows, не будут видны в *nix, и наоборот. Это связано с различной структурой файловой системы в различных реализациях библиотеки. Поэтому перед использованием токена в *nix обязательно необходимо выполнить его форматирование, как это показано выше.

Настройка браузера и почтового клиента для работы с Rutoken

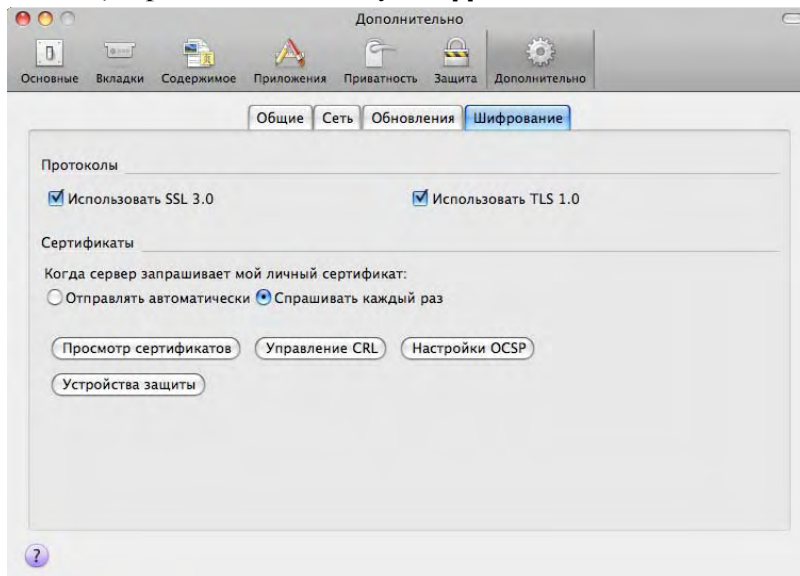
Чтобы настроить Firefox и Thunderbird для работы с Rutoken, необходимо посредством *nix-библиотеки PKCS11 записать на токен сертификат (например, как показано выше):

Важная информация

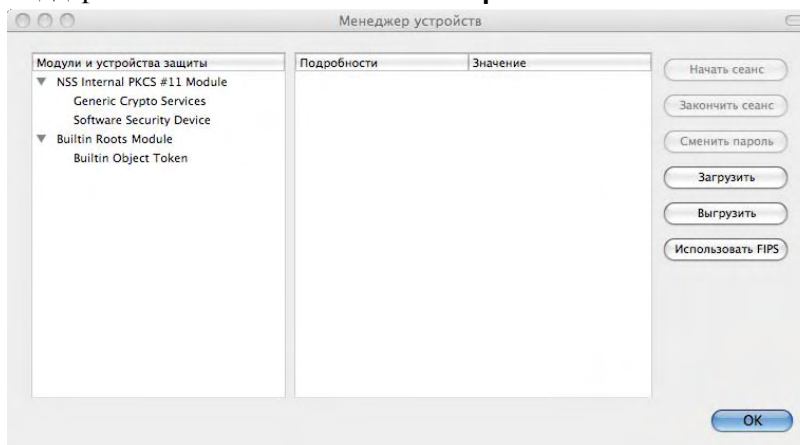
Перед запуском Firefox (и Thunderbird) необходимо, чтобы менеджер ресурсов **pcsc-lite – pcscd** – был запущен и выполнялся. Для этого подсоедините токен к USB-порту, либо настройте автоматический запуск **pcscd** при старте системы.

Настройка Firefox

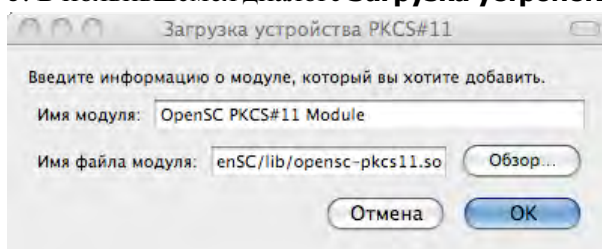
1. Откройте настройки Firefox: (**Firefox | Настройки...**). Далее выберите пункт **Дополнительно**, перейдите на вкладку **Шифрование** и нажмите на кнопку **[Устройства защиты]**:



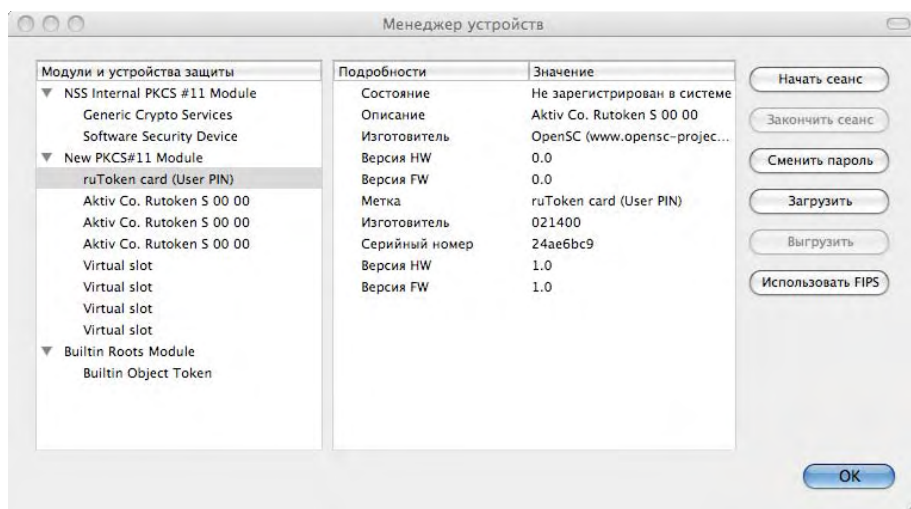
2. В окне **Менеджера устройств** нажмите на кнопку **[Загрузить]** для загрузки библиотеки поддержки PKCS#11 из комплекта **OpenSC**:



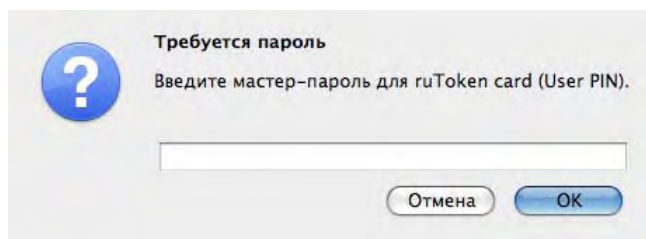
3. В появившемся диалоге **Загрузка устройства PKCS#11** нажмите на кнопку **[OK]**:



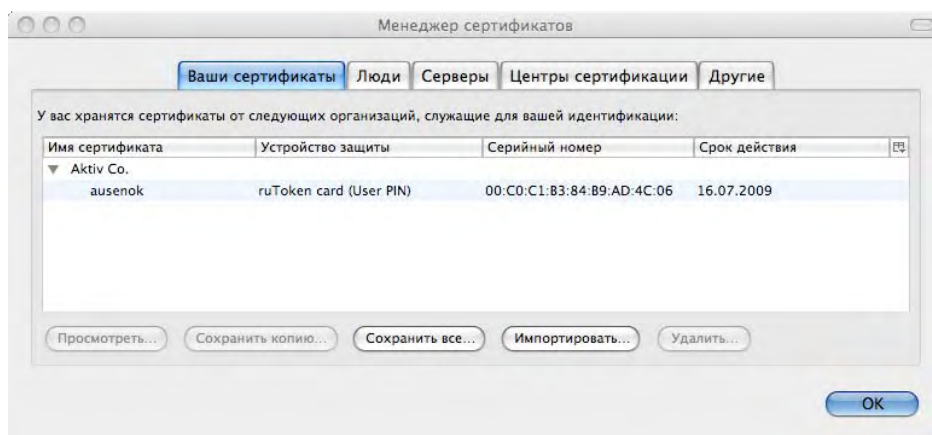
4. В окне **Менеджера устройств** задайте **Имя модуля**. В качестве имени укажите путь до файла **opensc-pkcs11.so**: **/Library/OpenSC/lib/opensc-pkcs11.so** (если использовался комплект SCA, при сборке вручную возможны другие варианты). Нажмите на кнопку **[OK]**. Приведенный скриншот означает, что Rutoken был корректно распознан библиотекой **pkcs11**:



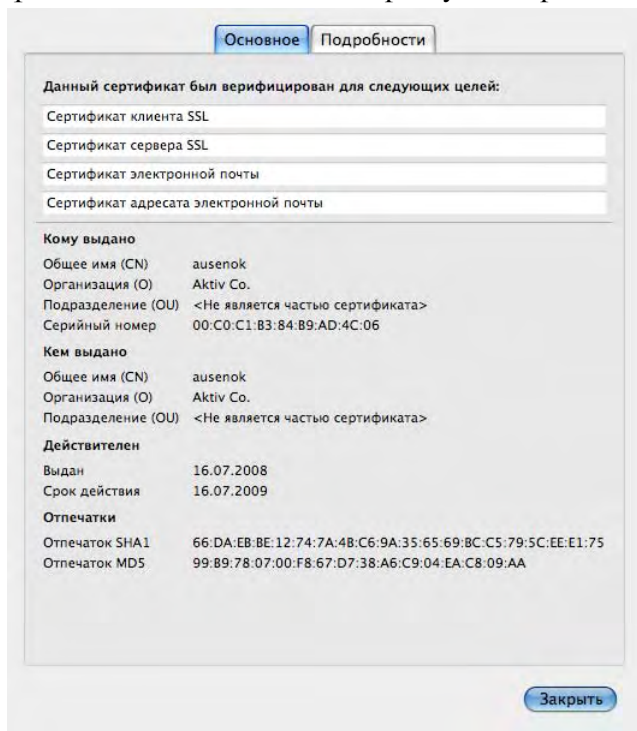
5. Нажмите на кнопку **[Начать сеанс]** и введите PIN-код пользователя Rutoken (по умолчанию: **12345678**) в появившемся окне:



6. Убедитесь, что поле **Состояние** в правой части окна **Менеджера устройств** изменилось на **Зарегистрирован в системе**, и нажмите на кнопку **[OK]**. Далее нажмите на кнопку **[Просмотр сертификатов]**, и перейдите во вкладку **Ваши сертификаты**:

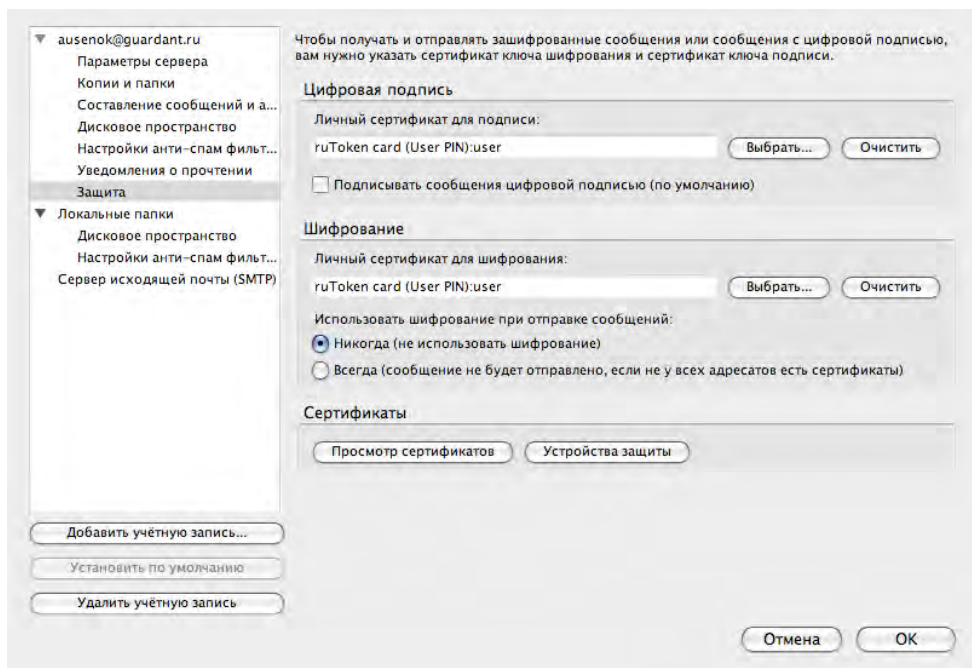


7. Нажмите на кнопку **[Просмотреть...]**, чтобы убедиться в корректности значений сертификата. После этого можно приступать к работе с защищенными веб-узлами.



Настройка Thunderbird

Настройка почтового клиента Thunderbird производится аналогично настройке Firefox. Единственное отличие заключается в том, что после просмотра и проверки сертификата необходимо установить его в качестве личного сертификата пользователя в настройках учетной записи (**Инструменты | Параметры учетной записи... | Защита**):



После этого можно обмениваться зашифрованной и/или подписанной почтой с собеседником, имеющим сертификат.

Дополнительные источники информации

При возникновении вопросов, на которые вам не удалось найти ответа в этой инструкции, рекомендуем обратиться к следующим дополнительным источникам информации:

WWW: <http://www.Rutoken.ru>

Web-сайт разработчика содержит большой объем справочной информации об электронных идентификаторах Rutoken.

Служба технической поддержки:

e-mail: hotline@Rutoken.ru

тел. +7(495)925-77-90