ESMART®

ESMART Token – PKCS#11 Java API

Содержание

1. Общая информация

Java API предназначено для вызова некоторых функций библиотеки PKCS#11 из Java. Вызовы функций библиотеки PKCS#11 осуществляются через технологию JNI (Java Native Interface). Помимо Java приводится пример использования данной библиотеки в JavaScript с использованием технологии Java Applet.

2. Требования к операционной системе

- *Windows XP* — *32 и 64 бита;*
- *Windows Vista* — *32 и 64 бита;*
- *Windows 7* — *32 и 64 бита;*
- *Windows 8 или 8.1* — *32 и 64 бита;*
- *Windows 10* — *32 и 64 бита;*
- *Windows Server 2003 / 2008 / 2012* — *32 и 64 бита;*
- *Linux (SUSE, AltLinux и др)* — *32 и 64 бита;*
- *Mac OS X 10.7 и выше*[1] — *32 бита.*

3. Требования к Java-машине

*Java SE 1.6 и выше, для 64-битных машин требуется использовать 64-битные библиотеки, их требуется положить в директорию **SDK\Java\bin**. Последние версии библиотек можно найти на сайте www.esmart.ru.*

4. Настройка браузеров

4.1 Internet Explorer

*Откройте **Свойства обозревателя** вкладка **Безопасность**.*

*В окошке выберите **Надежные узлы** и нажмите кнопку **Другой** в нижней части окна, чтобы изменить уровень безопасности.*

*Выберите в списке **Сценарии › Выполнять сценарии приложений Java** и отметьте **Включить**.*

4.2 Firefox

*В верхней части окна браузера нажмите **Firefox**, затем перейдите в раздел **Дополнения**. Откроется вкладка **Диспетчер дополнений**.*

*На вкладке **Диспетчер дополнений** выберите **Подключаемые модули**.*

*Выберите подключаемый модуль **Java (TM) Platform**. Нажмите кнопку **Включить** (если на кнопке отображается надпись **Выключить**, то поддержка Java уже включена).*

4.3 Safari

*Откройте меню **Safari › Параметр** . Перейдите на вкладку **Безопасность** . Установите флажок **Разрешить Java**.*

---

[1] *Для запуска Java 7 на Mac OS X требуется 64-битный браузер (например, Safari или Firefox). 32-разрядные браузеры, такие как Chrome, не поддерживают Java 7 на платформе macOS.*

4.4 Opera

Браузер Opera для Windows не использует Java на локальной машине, а уже содержит встроенную Java-машину. Дополнительная информация представлена на сайтах http://java.com и http://www.opera.com.

5. Установка в Windows

*Перед использованием установите необходимые библиотеки с помощью инсталлятора из папки **Windows\installer**. Установка при помощи инсталлятора описана в руководстве **ESMART PKI Client – Руководство администратора**.*

*При запуске программы-инсталлятора библиотека **EsmartToken_Javalib.dll**, реализующая JNI, копируется в папку **X:\Windows\System32** (или любую другую, прописанную в системной переменной PATH). Редактирование реестра и копирование файлов вручную не требуются.*

*Если требуется установка вручную, скопируйте dll-библиотеки из папки **SDK\Java\bin** в папку **X:\Windows\System32.** Запустите файлы редактирования реестра **esmarttoken x86.reg** или **esmarttoken x64.reg** из папки Windows\installer\pkcs11\registry files в зависимости от типа установленной операционной системы.*

Дополнительно требуется установка Распространяемого пакета Microsoft Visual C++ 2010 (x86)[2]

6. Установка в Linux

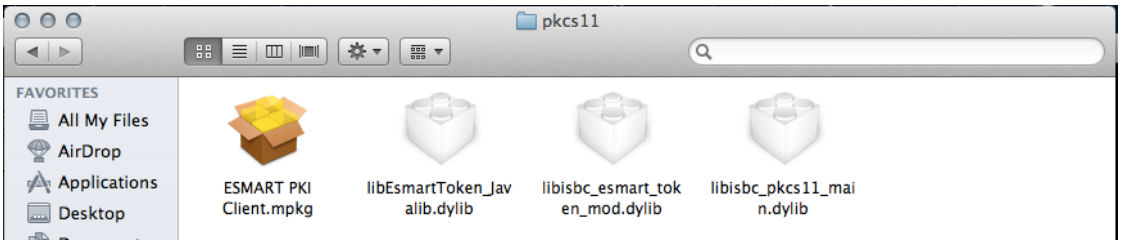
*Перед использованием установите библиотеки PKCS#11 с помощью rpm-пакета **Linux/pkcs11/isbc-pkcs11-x.x.x-x.i586.rpm:***

```
rpm –ivh isbc-pkcs11-x.x.x-x.i586.rpm
```

*Если требуется установка вручную, скопируйте so-файлы из папки **SDK/Java/bin** в папку **/usr/lib**, включая **libEsmartToken_Javalib.so**, реализующую интерфейс JNI.*

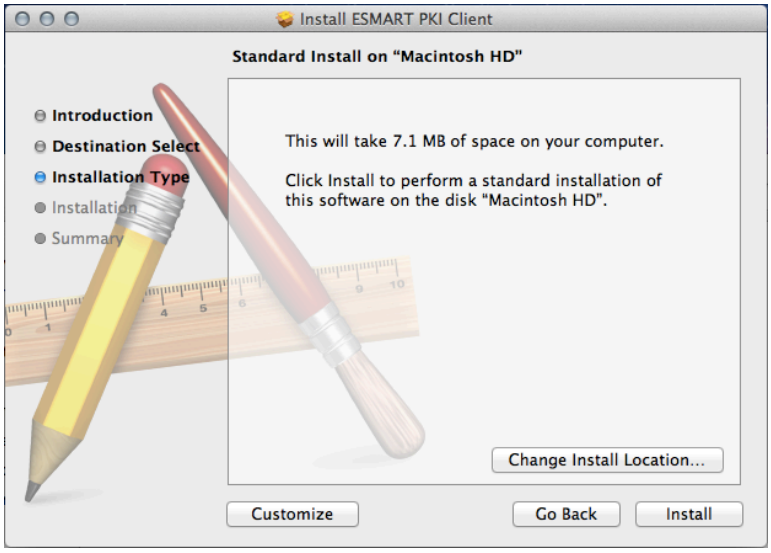
7. Установка в Mac OS

Откройте папку MacOS/pkcs11 и запустите программу-инсталлятор ESMART PKI Client.mpkg. Следуйте подсказкам.



*Укажите место установки, нажав **Change Install Location...** или оставьте значение по умолчанию.*

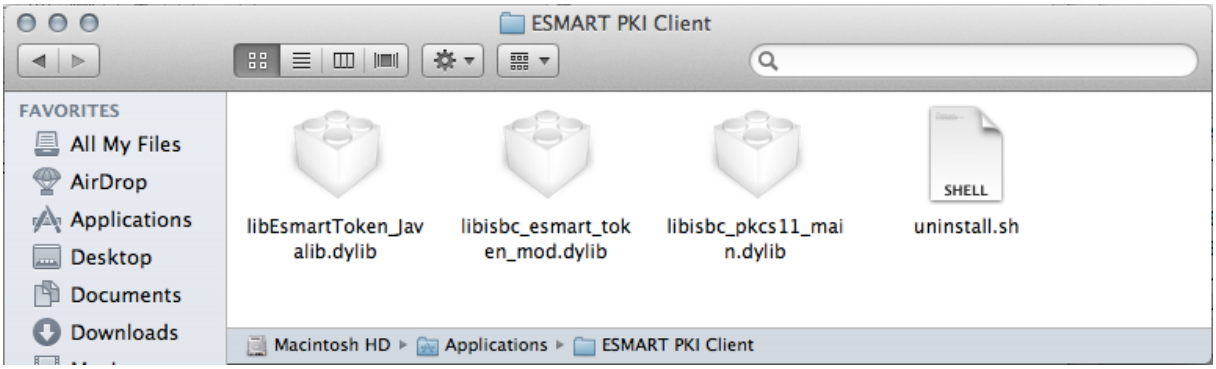
[2] *https://www.microsoft.com/ru-RU/download/details.aspx?id=5555*



Дождитесь окончания установки и сообщения ***Установка успешно завершена*** *(**The Installation was successful**).*

Если при установке было выбрано место установки по умолчанию, в разделе Application (Приложения) появится папка ESMART PKI Client, содержащая файлы:

- *libisbc_esmart_token_mod.dylib;*
- *libesmart_token_gost_mod.dylib;*
- *libisbc_pkcs11_main.dylib;*
- *libEsmartToken_Javalib.dylib;*
- *uninstall.sh.*



8. Состав Java SDK

- ***SDK\Java\bin*** *– содержит пример приложения для Java, демонстрирующий работу Java API.*
  - ***ConsoleDemo.bat*** *– запускает приложение для Windows.*
  - ***ConsoleDemo*** *– запускает приложение под Linux.*
- ***SDK\Java\conf*** *– содержит конфигурационный файл системы логирования. Также для примера приложены тестовый сертификат в формате PKCS#12 (пароль 123) и соответствующий корневой сертификат ca.crt в формате DER.*
- ***SDK\Java\javadoc*** *– содержит описание API.*
- ***SDK\Java\repo*** *– содержит jar-файлы библиотек, используемых в данном API.*
- ***SDK\Java\src*** *– содержит пример приложения для работы с данным API, а также пример Java Applet.*

- ***SDK\Java\webapps*** *– содержит файлы для публикации на WEB-сервере и для использования данного API в JavaScript.*

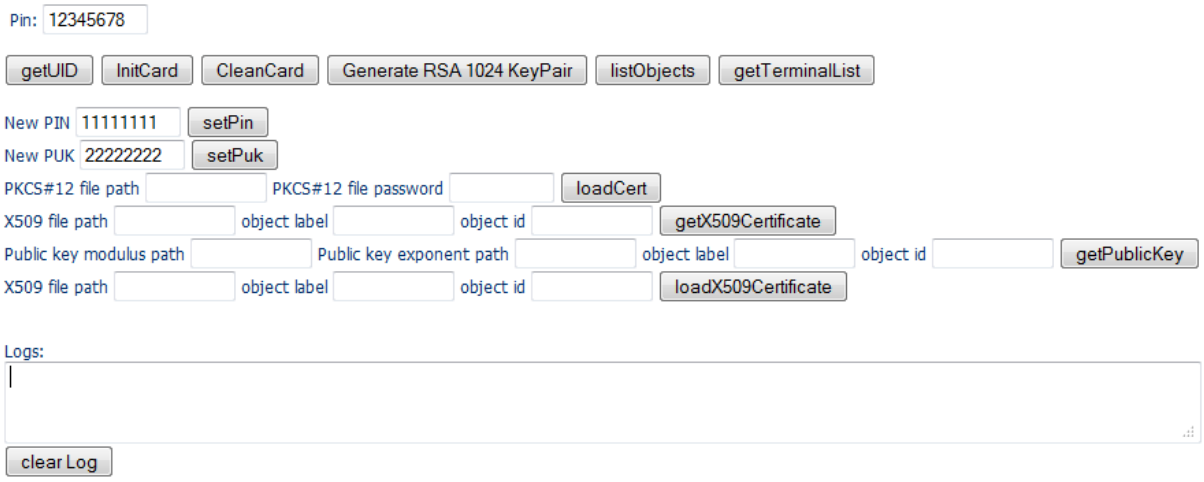
9. JavaScript

Пример Java Applet уже скомпилирован в SDK\Java\webapps\esmarttoken-2.0.jar и подписан тестовым сертификатом. Для использования в рабочих проектах необходима подпись действительным сертификатом.

Пример вызова API из JavaScript приведен в файле ***webapps\applet.html****.*

Демонстрационная страница на базе апплета размещена по адресу:

http://www.isbc.ru/esmarttest/applet.html



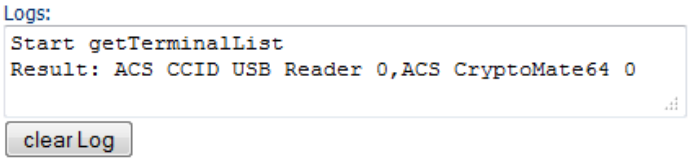
Элементы управления:

Pin	*Поле для ввода ПИН-кода карты*
getUID	*Получить UID карты*
InitCard	*Инициализировать карту*
CleanCard	*Очистить карту*
Generate RSA 1024 KeyPair	*Генерировать на карте ключевую пару RSA длиной 1024 байта*
listObjects	*Вывести список объектов на карте*
getTerminalList	*Вывести список подключенных считывателей*
New PIN	*Поле для ввода нового ПИН-кода*
setPin	*Сменить ПИН-код*
New PUK	*Поле для ввода нового PUK-кода*
setPuk	*Сменить PUK-код*
PKCS#12 file path	*Задать путь к файлу PKCS#12, например, к тестовому сертификату SDK\Java\conf\clientTest2.p12*
PKCS#12 file password	*Поле ввода пароля к файлу PKCS#12 (пароль для тестового файла: 123)*
loadCert	*Загрузить сертификаты из файла PKCS#12 (.p12) на смарт-карту*
X509 file path	*Задать путь к локальному файлу, в который будет сохранен сертификат, записанный на карте*
object label	*Название объекта (можно получить командой listObjects)*
object id	*Идентификатор объекта (можно получить командой listObjects)*

getX509Certificate	*Сохранить сертификат на карте в локальный файл*
Public key modulus path	*Задать путь к локальному файлу, в который будет записан модуль открытого ключа*
Public key exponent path	*Задать путь к локальному файлу, в который будет записана экспонента открытого ключа*
getPublicKey	*Сохранить модуль и экспоненту открытого ключа, записанного на карту, в локальные файлы*

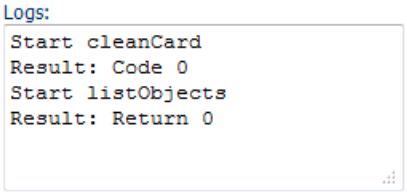
9.1 Просмотр списка считывателей

*Нажмите **getTerminalList** для просмотра списка подключенных считывателей*

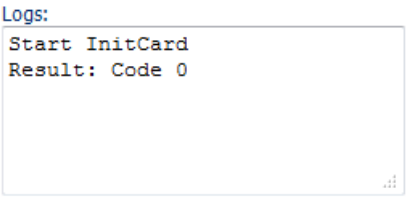


9.2 Очистка и инициализация карты

*Нажмите **CleanCard**, чтобы очистить карту, а затем **listObjects**.*

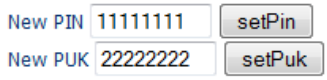


*Запустите **InitCard** для инициализации карты. Если PUK карты был изменен, при инициализации в поле **Pin** необходимо ввести действующий PUK-код.*



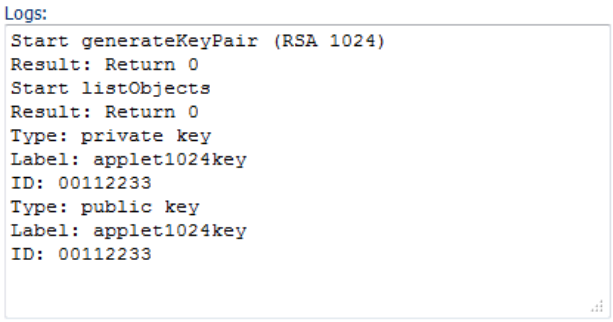
9.3 Смена PIN и PUK

*Введите в поле новый PIN или PUK, затем нажмите **setPin** или **setPuk** соответственно.*



9.4 Генерация ключевой пары

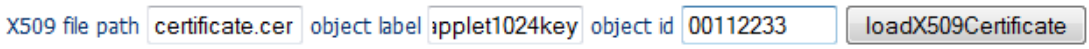
*Нажмите **generateKeyPair**, а затем **listObjects** для проверки результата выполнения операции.*



9.5 Запись сертификата на карту

Сертификат, полученный в Удостоверяющем центре, необходимо записать на карту.

*Сертификат должен быть в формате DER. Сертификаты, полученные в формате base64, можно переконвертировать при помощи OpenSSL (см. руководство **ESMART Token – PKCS11**).*



*Введите полный путь к сертификату, а также название и идентификатор соответствующей ключевой пары (длина **id** всегда должна быть чётным числом), нажмите **loadX509Certificate**. Проверьте наличие сертификата, вызвав **listObjects**.*

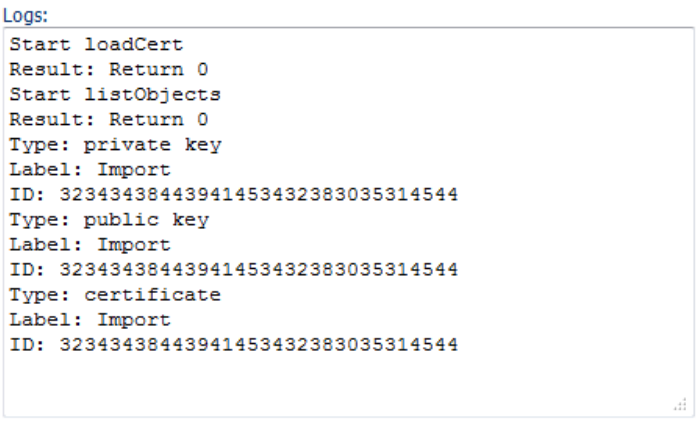
9.6 Импорт ключевой пары и сертификата

Из файла PKCS#12 можно импортировать на карту ключевую пару и сертификат одновременно. Файл PKCS#12 (.p12 или .pfx) обычно защищен паролем. Путь к файлу требуется вводить полностью, например, C:\certs\ClientTest2.p12.

*Нажмите **loadCert**, а после выполнения операции **listObjects** для получения информации о загруженных объектах. При импорте из PKCS#12 на карте записываются:*

- *Открытый ключ;*
- *Закрытый ключ;*
- *Сертификат.*

Обращаем внимание, что все три объекта имеют одинаковые название и идентификатор.



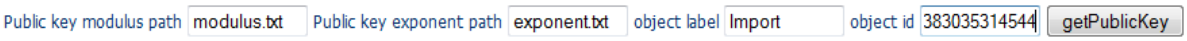
*Обратите внимание на поля **Label** и **ID**, эти значения необходимы для экспорта сертификата, а также модуля и экспоненты открытого ключа.*

9.7 Экспорт сертификата с карты

Сертификат, записанный на карту, можно сохранить в файл, например, чтобы отправить по электронной почте. Обычно, сертификаты имеют разрешение .cer.

Введите полный путь к файлу и его название, например, C:\certs\certificate.cer

9.8 Экспорт модуля и экспоненты открытого ключа



*Введите полный путь к файлам, в которые будут сохраняться модуль и экспонента открытого ключа и нажмите **getPublicKey**.*

10. Удаление компонентов

*При использовании автоматической установки в Windows воспользуйтесь панелью управления Windows, раздел **Удаление программ**. Если использовалась ручная установка, удалите файлы библиотек .dll, а также запустите файлы изменения реестра **remove esmarttoken x86.reg** или **remove esmarttoken x64.reg**, входящие в комплект установки.*

Список библиотек для удаления в Windows:

- *EsmartToken_Javalib.dll*
- *esmart_token_gost_mod.dll;*
- *isbc_esmart_token_mod.dll*
- *isbc_pkcs11_main.dll.*

Список библиотек для удаления в Linux:

- *libEsmartToken_Javalib.so;*
- *libisbc_esmart_token_mod.so;*
- *libesmart_token_gost_mod.so;*
- *libisbc_pkcs11_main.so.*

Список библиотек для удаления в Mac OS X в папке Приложения/Applications:

- *libEsmartToken_Javalib.dylib;*
- *libisbc_esmart_token_mod.dylib;*
- *libesmart_token_gost_mod.dylib;*
- *libisbc_pkcs11_main.dylib.*

Опытным пользователям Mac OS X рекомендуется удалить компонент, запустив в консоли:

```
sudo /Applications/ESMART\ PKI\ Client/uninstall.sh
```