JaCarta для Linux

Руководство по внедрению

Аннотация

Настоящий документ представляет собой руководство по внедрению и использованию электронных ключей JaCarta с апплетом Laser в среде Linux. Электронные ключи JaCarta можно использовать в большинстве 32- и 64-битных операционных систем Linux.

Следование приведённым в настоящем документе инструкциям является верным, но не всегда единственно возможным способом достижения цели. В этом смысле эти инструкции носят рекомендательный характер.

Для эффективного внедрения и управления электронными ключами JaCarta в среде Linux требуется квалифицированный системный администратор.

Вопросы или пожелания по содержанию настоящего документа направляйте по адресу techwriters@aladdin-rd.ru.

Будем благодарны за конструктивные замечания и ответим на возникшие вопросы.

За технической поддержкой обращайтесь на веб-сайт ЗАО «Аладдин Р. Д.» по адресу http://www.aladdin-rd.ru/support/index.php.

Версия	2.0
Редакция от	30.05.2014
Листов	24

Телефон +7 (495) 223-00-01 • Факс +7 (495) 646-64-40 • aladdin@aladdin-rd.ru • www.aladdin-rd.ru

Содержание

1. Введение

Чтобы использовать электронные ключи JaCarta в среде Linux, необходимо установить:

1. программное обеспечение, которое включает библиотеки, осуществляющие взаимодействие приложений с электронными ключами JaCarta через интерфейс PKCS#11;
2. ПО управления электронными ключами, которое позволяет изменять пароль пользователя, пароль администратора, пароль цифровой подписи и пароль разблокировки цифровой подписи электронных ключей JaCarta (см. табл. 1).

Табл. 1

Типы паролей электронных ключей JaCarta

Тип пароля	Описание
Пароль пользователя	Обеспечивает доступ к электронному ключу JaCarta на уровне пользователя.
Пароль администратора	Обеспечивает доступ к электронному ключу JaCarta на уровне администратора, в том числе позволяет разблокировать заблокированный пароль пользователя, который был заблокирован при превышении допустимого количества неверных попыток ввода.
Пароль цифровой подписи	Дополнительный пароль для использования цифровой подписи, который может быть назначен на этапе персонализации электронного ключа JaCarta.
Пароль разблокировки цифровой подписи	Позволяет разблокировать пароль цифровой подписи, который был заблокирован при превышении допустимого количества неверных попыток ввода.

Подробное описание указанных выше паролей находится в документе «JC-Client. Руководство пользователя» и «JC-Client. Руководство администратора».

ПО управления электронными ключами представлена в двух вариантах:

- ПО с графическим пользовательским интерфейсом;
- утилита командной строки.

Установка программного обеспечения и использование электронных ключей JaCarta в среде Linux позволит осуществлять следующие действия:

- аутентификация пользователя по цифровому сертификату, хранящемуся в электронном ключе, при работе через браузер (в рамках протокола SSL/TLS);
- шифрование и цифровая подпись при использовании электронной почты;
- взаимодействие с другими приложениями, которые поддерживают интерфейс PKCS#11.

2. Описание пакетов установки

2.1. Утилита с графическим интерфейсом

Табл. 2

Пакеты установки утилиты с графическим интерфейсом

Имя файла	Описание
IDProtectClient610.12_ALT_x86.run	Сценарий установки ПО с графическим интерфейсом для использования JaCarta в среде Linux для 32-битных платформ.
IDProtectClient610.12_ALT_x64.run	Сценарий установки ПО с графическим интерфейсом для использования JaCarta в среде Linux для 64-битных платформ.

ПО с графическим интерфейсом работает как на 32-, так и на 64-битных версиях дистрибутивов, основанных на Debian и Red Hat.

2.2. Утилита командной строки

Табл. 3

Пакет установки консольной версии программного обеспечения

Имя файла	Описание
IDPClientDB_user.xml	Конфигурационный XML-файл.
aseInstall	Сценарий установки программного обеспечения для использования JaCarta в среде Linux.
IDPClientDB.xml	Конфигурационный XML-файл.
README	Файл справки (на английском языке).
ase-pin-tool	Утилита командной строки, позволяющая изменять пароль пользователя, пароль администратора, пароль цифровой подписи, пароль разблокировки цифровой подписи, а также выполнять другие операции.
libASEP11.so	Реализация интерфейса PKCS#11.

Утилита командной строки работает только на 32-битных версиях дистрибутивов, основанных на Red Hat.

3. Системные требования

Перед установкой программного обеспечения для использования электронных ключей JaCarta в среде Linux удостоверьтесь в том, что компьютер соответствует минимальным требованиям.

Табл. 4

Системные требования

Поддерживаемые операционные системы	○ Дистрибутивы, основанные на Red Hat (32- и 64-битные платформы) ○ Дистрибутивы, основанные на Debian (32- и 64-битные платформы)
Поддерживаемые браузеры	Firefox (версии 3 и более поздних версий)
Поддерживаемые почтовые клиенты	Thunderbird (версии 3 и более поздних версий)
Поддерживаемые модели электронных ключей	Смарт-карты и USB-токены JaCarta PKI, JaCarta FLASH, JaCarta FLASH/ГОСТ/PKI, JaCarta PRO/PKI и JaCarta ГОСТ/PKI
Необходимые аппаратные средства	○ USB-порт (для USB-токенов JaCarta) ○ Считыватель смарт-карт (для смарт-карт JaCarta)
Необходимые драйверы и библиотеки	○ Для CCID-совместимых считывателей и USB-токенов — драйвер CCID ○ Для считывателей, не соответствующие спецификации CCID — драйверы для таких считывателей

В настоящем документе все действия описаны на примере дистрибутива ALT Linux 6/Astra Linux (кроме утилиты ase-pin-tool, стр. 16). Для других дистрибутивов указанные ниже команды и набор библиотек для работы со смарт-картами и считывателями смарт-карт могут отличаться. В таких случаях обращайтесь к справочным руководствам соответствующих дистрибутивов.

4. Установка и примеры использования

4.1. Порядок установки

Установка производится в два этапа:

1. предварительная установка библиотек для взаимодействия операционной системы со смарт-картами и считывателями смарт-карт;
2. установка утилиты управления JaCarta.

4.2. Предварительная установка библиотек для работы со смарт-картами и считывателями смарт-карт

Для работы утилиты управления JaCarta необходимо установить следующие компоненты:

- PC/SC Lite — промежуточный слой для обеспечения доступа к смарт-картам по стандарту PC/SC, пакет pcsc-lite.
- Библиотеки ccid и libusb для работы с USB-ключами, смарт-картами и считывателями смарт-карт.

Состав указанного выше ПО зависит от типов используемых устройств. Если будут использоваться и смарт-карты, и USB-токены, и при этом считыватель смарт-карт стандарта PC/SC не поддерживает CCID, то потребуется установить и драйвер считывателя, и драйвер CCID.

Для установки указанных библиотек в зависимости от используемой версии Linux выполните следующую команду (см. табл. 5 и рис. 1).

Табл. 5

Предварительная установка необходимых компонентов

ALT Linux 6	`sudo apt-get install libusb pcsc-lite ccid`
Astra Linux	`sudo apt-get install libccid pcscd libpcsclite1`

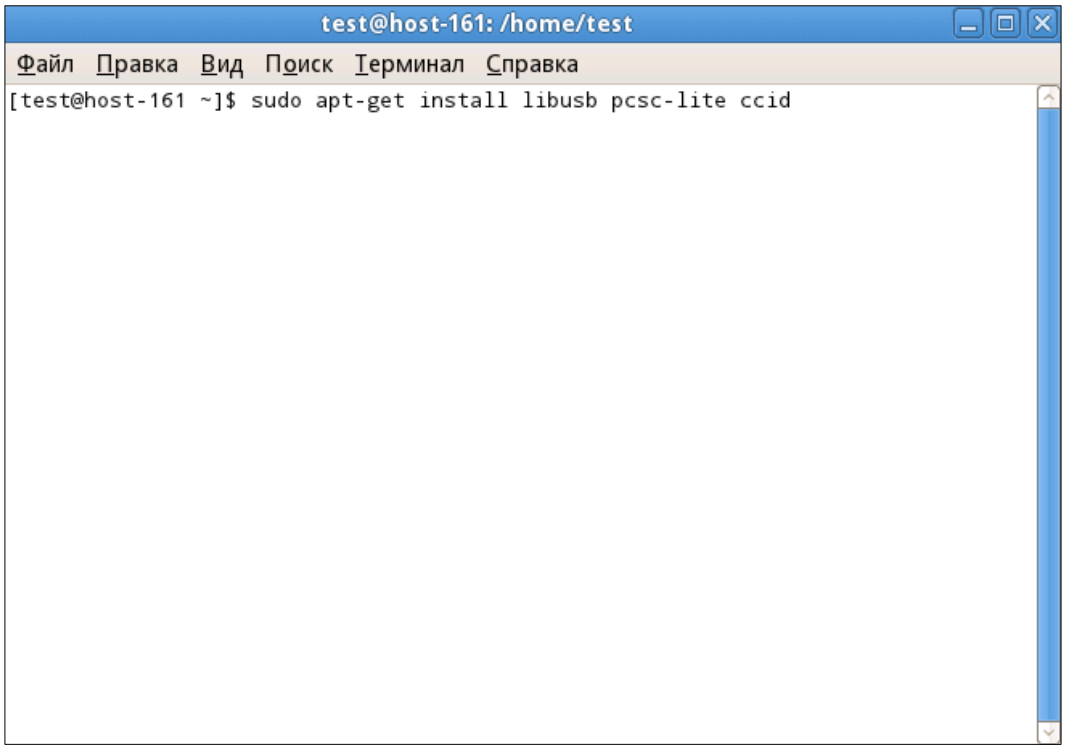

Рис. 1 – Окно командной строки (терминала)

Пакеты *libusb*, *pcsc-lite* и *ccid* устанавливаются из стандартного репозитория, включённого по умолчанию. Данный набор пакетов необходим для работы смарт-карт и считывателей смарт-карт в операционной системе ALTLinux. Набор пакетов для других ОС может быть иным.

4.3. Программное обеспечение с графическим интерфейсом

УСТАНОВКА

Для установки ПО с графическим интерфейсом, выполните следующие действия:

1. В домашней директории **/home/user/**, где **user** — имя текущего пользователя, создайте любую директорию, например **ID**, и поместите в неё установочный пакет — **IDProtectClient610.12_ALT_x86.run** или **IDProtectClient610.12_ALT_x64.run** в зависимости от разрядности установленной операционной системы.
2. Параметру, определяющему права доступа пользователей к установочному пакету, присвойте значение 777, выполнив команду:

```
sudo chmod 777 /home/user/ID/IDProtectClient610.12_ALT_x86.run
```

3. Запустите установочный пакет командой:

```
sudo /home/user/ID/IDProtectClient610.12_ALT_x86.run
```

4. В открывшемся окне нажмите кнопку **Next** (Далее).

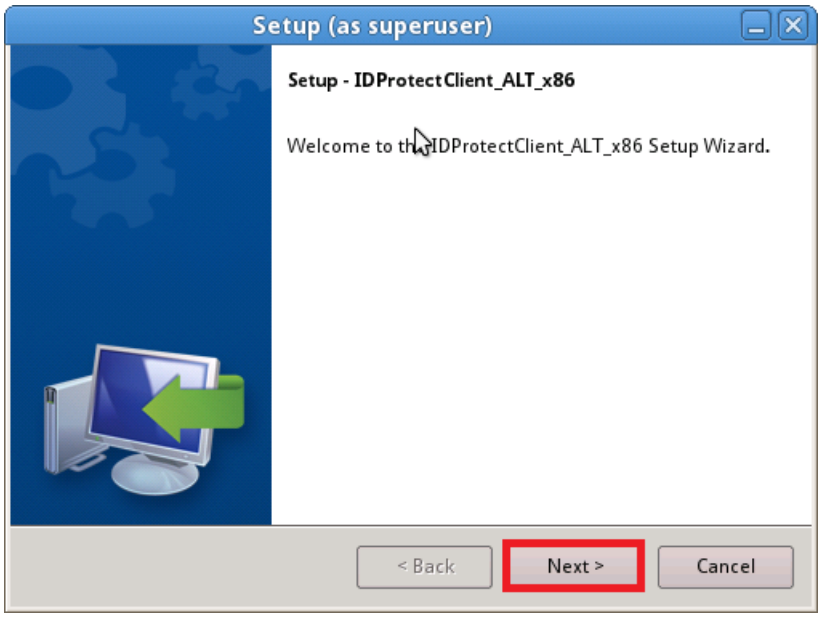

Рис. 2 – Окно приветствия мастера установки

5. Укажите путь установки как показано на рисунке и нажмите кнопку **Next** (Далее).

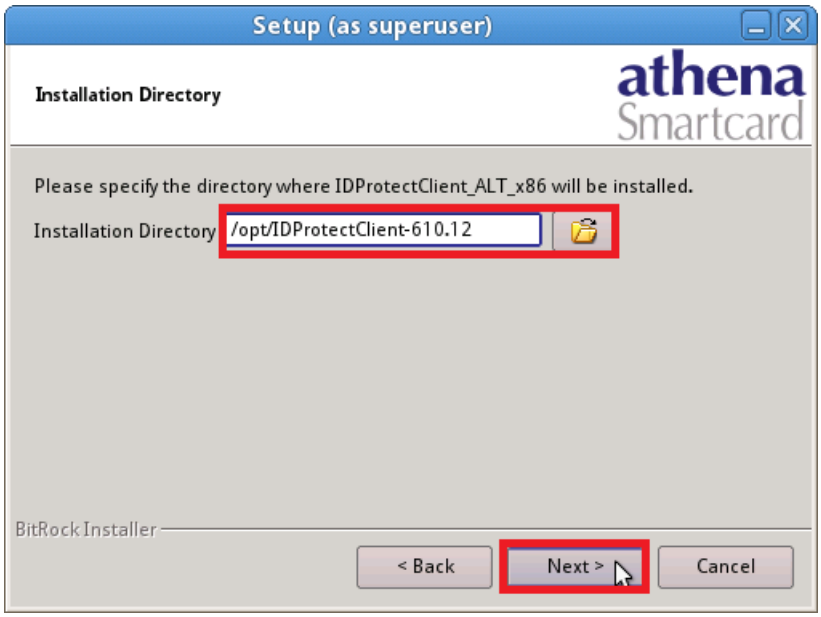

Рис. 3 – Путь установки

6. В зависимости от операционной системы выполните следующие действия.

- Если вы устанавливаете ПО в операционной системе ALT Linux 6, переходите к шагу 7 настоящей процедуры.

- Если вы устанавливаете ПО в операционной системе Astra Linux, выберите компоненты устанавливаемого ПО (см. рис. 4 и табл. 6) и нажмите **Next** (Далее).

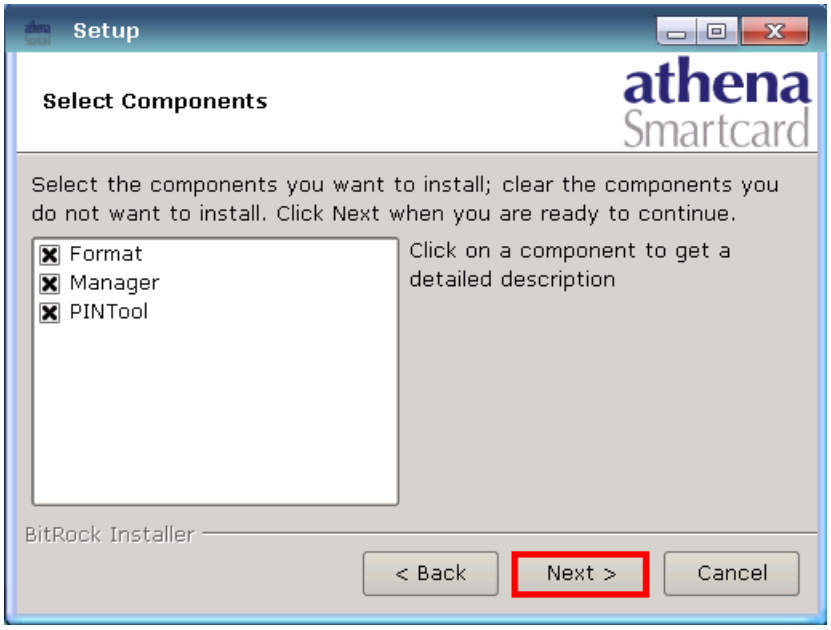

Рис. 4 – Выбор компонентов установки

Табл. 6

Компоненты установки

Компонент	Описание
Format	Утилита, позволяющая персонализировать электронные ключи JaCarta (подробнее см. документ «JC-Client. Руководство администратора»).
Manager	Утилита, позволяющая управлять сертификатами в памяти электронных ключей JaCarta (подробнее см. документ «JC-Client. Руководство администратора»).
PINTool	Утилита, позволяющая разблокировать и изменять пароль пользователя и пароль цифровой подписи JaCarta (подробнее см. документ «JC-Client. Руководство администратора»).

7. В открывшемся окне нажмите кнопку **Next** (Далее).

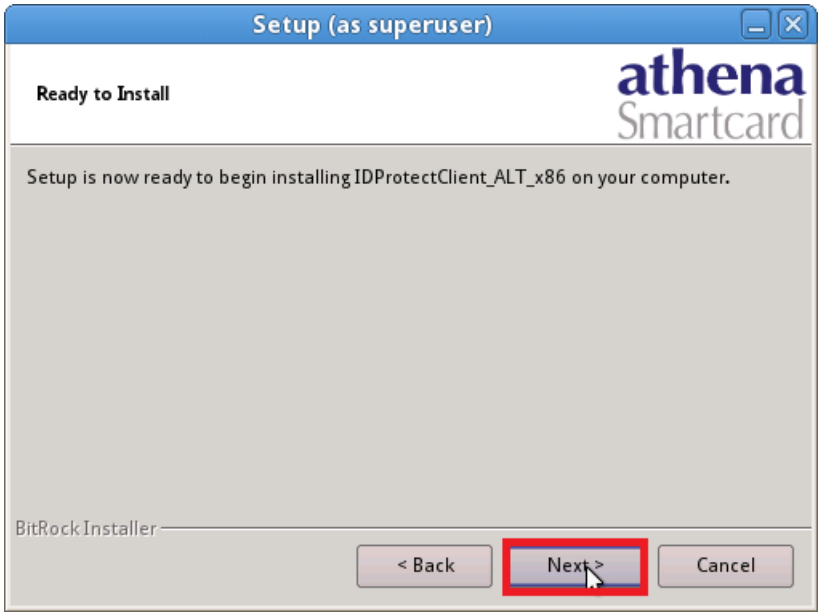

Рис. 5 – Окно готовности к установке

Установка займёт некоторое время.

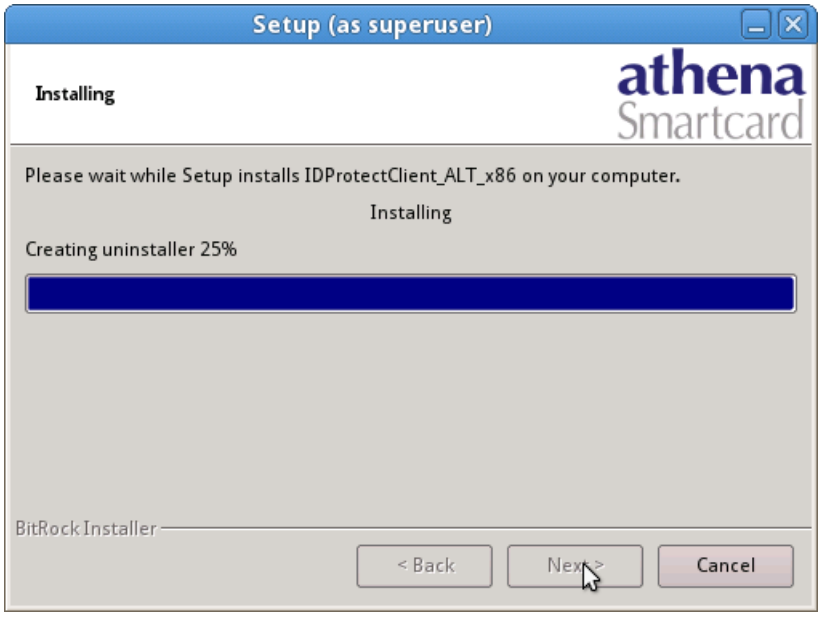

Рис. 6 – Процесс установки

8. По завершении установки нажмите кнопку **Finish** (Готово), после чего дождитесь перезагрузки компьютера.

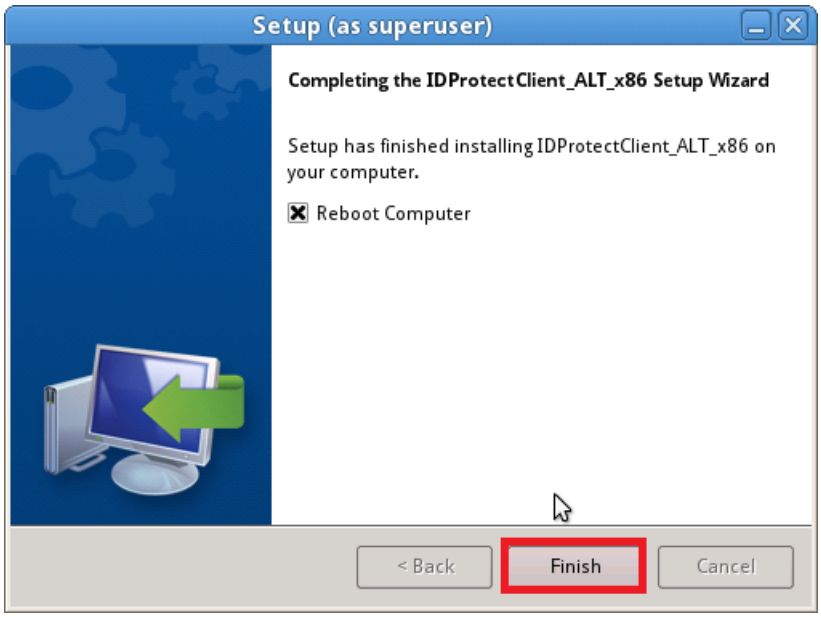

Рис. 7 – Окно завершения установки

ПРОВЕРКА РАБОТОСПОСОБНОСТИ

Чтобы убедится в том, что установка прошла успешно, выполните следующие действия.

1. Подсоедините электронный ключ JaCarta к компьютеру.
2. В зависимости от используемой версии Linux запустите установленное приложение следующим способом (см. табл. 7)

Табл. 7

Запуск установленного приложения

ALT Linux 6	В меню **Applications** (Приложения) выберите **Other** (Прочие) > **IDProtect PINTool** (см. рис. 8).
Astra Linux	Из стартового меню выберите **Прочие** > **IDProtect PINTool** (см. рис. 9).

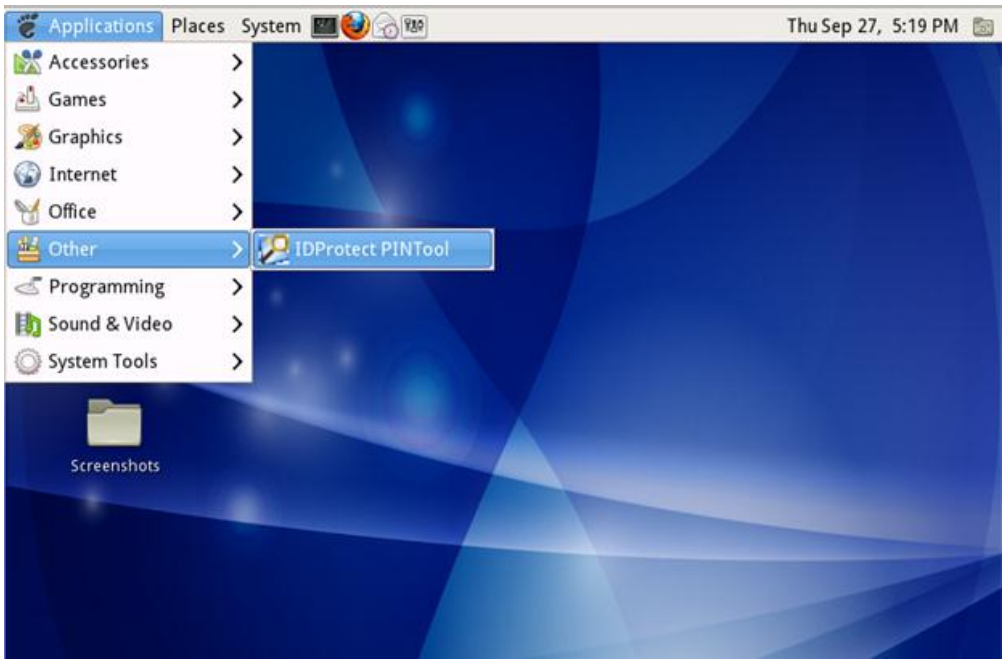

Рис. 8 – Запуск приложения управления электронными ключами JaCarta (на примере ALT Linux 6)

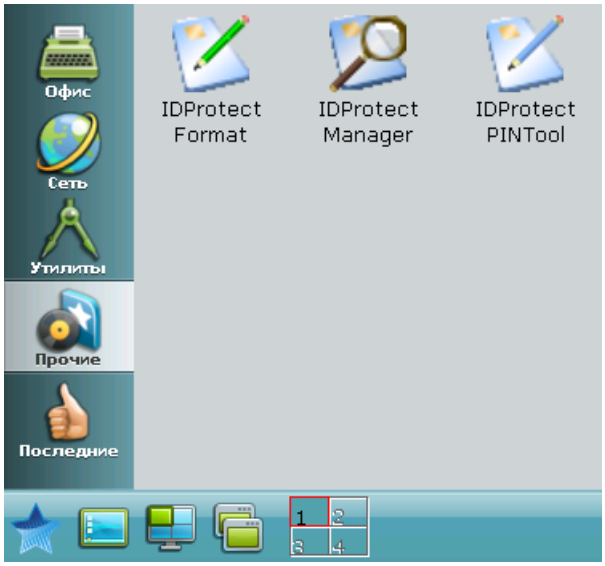

Рис. 9 - Запуск приложения управления электронными ключами JaCarta (на примере Astra Linux)

3. Убедитесь, что в приложении отображается подключенное устройство JaCarta.

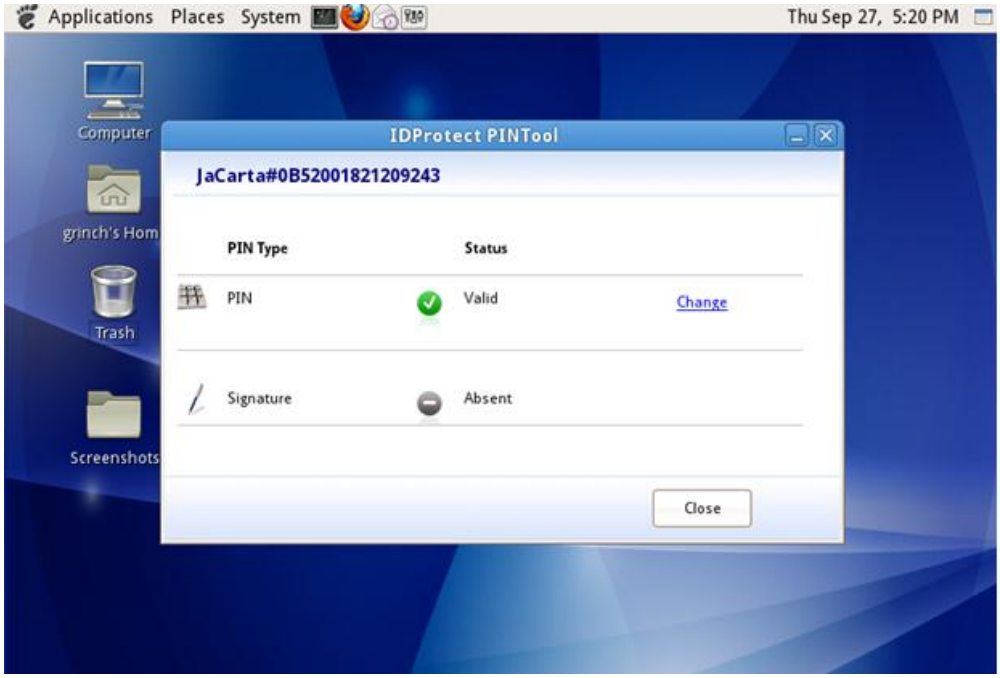

Рис. 10 – Окно приложения управления электронными ключами JaCarta

ПРИМЕР ИСПОЛЬЗОВАНИЯ

1. Запустите установленное приложение (см. п. «Проверка работоспособности»).
2. В открывшемся окне щёлкните **Change** (Изменить).

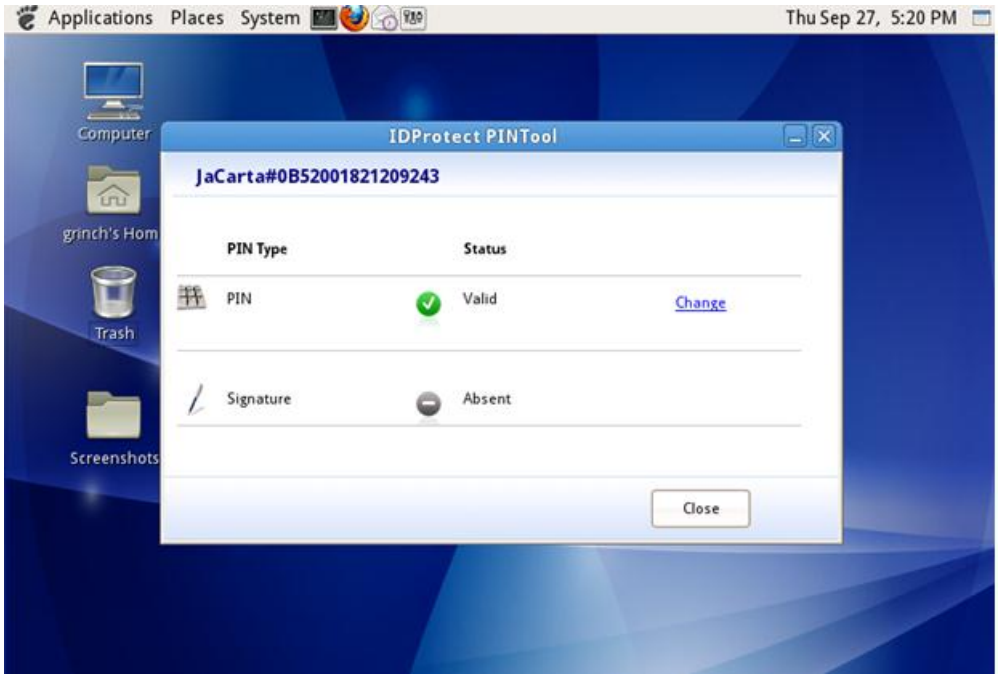

Рис. 11 – Окно приложения управления электронными ключами JaCarta

3. В следующем окне в поля **Current user pin** (Текущий пароль пользователя), **New user pin** (Новый пароль пользователя), **Confirm new pin** (Подтверждение нового паро-

ля) введите соответственно текущий пароль пользователя JaCarta, новый пароль пользователя JaCarta и подтверждение нового пароля пользователя JaCarta, после чего нажмите кнопку **Change** (Изменить).

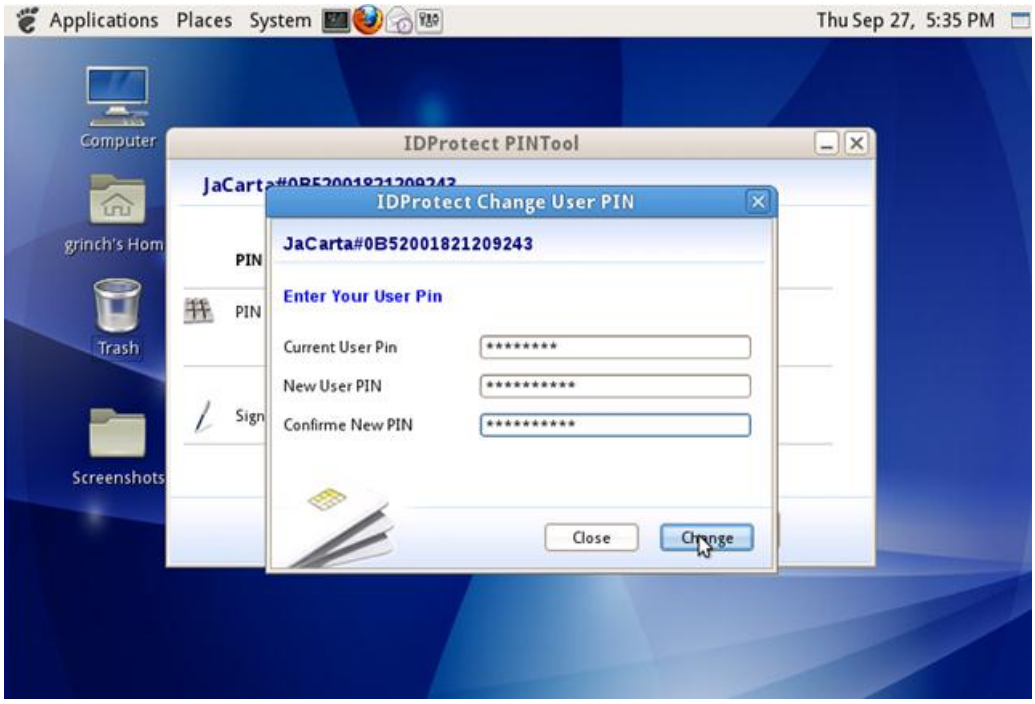

Рис. 12 – Смена пароля пользователя электронного ключа JaCarta

4. В отобразившемся окне нажмите **ОК.**

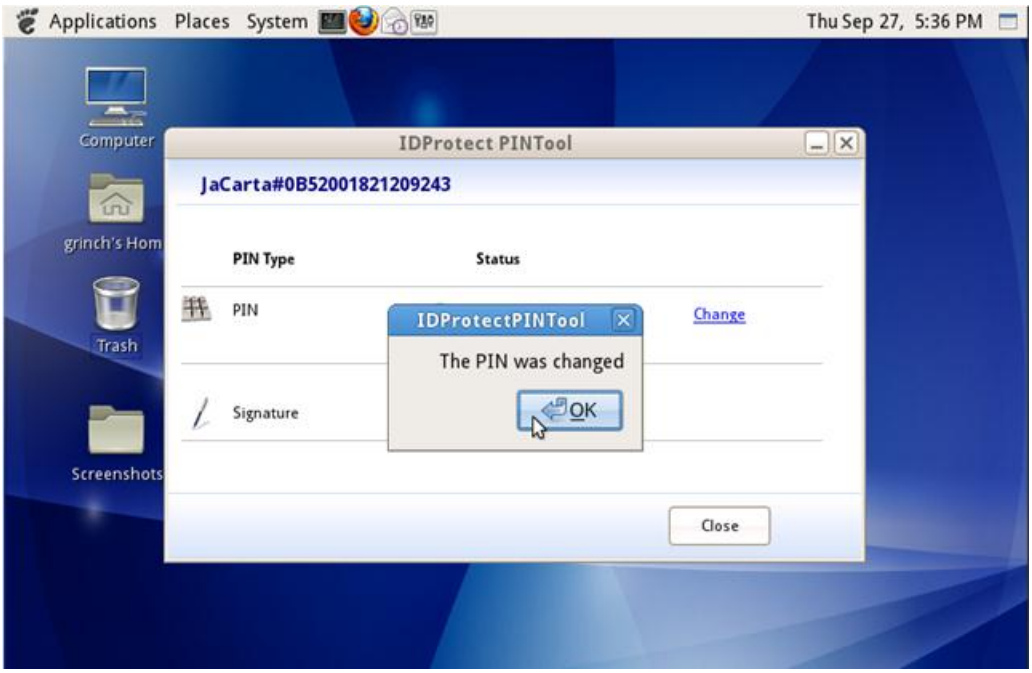

Рис. 13 – Подтверждение смены пароля пользователя электронного ключа JaCarta

4.4. Консольная версия программного обеспечения

УСТАНОВКА

Чтобы установить консольную версию ПО для использования JaCarta в среде Linux, выполните следующие действия.

1. Скопируйте файлы дистрибутива в любую папку на жёстком диске.
2. В командной строке из папки с файлами библиотеки выполните сценарий **aseInstall**, используя следующую команду:

```
sh aseInstall
```

3. Убедитесь в отсутствии сообщений об ошибках (кроме случаев обновления, когда отображаются сообщения о существовании ранее установленных файлов — такие сообщения можно игнорировать).

Утилита работает только на 32-битных версиях Linux-дистрибутивов, основанных на Red Hat.

ПРОВЕРКА РАБОТОСПОСОБНОСТИ

В состав дистрибутива ПО входит утилита командной строки **ase-pin-tool.** Данная утилита позволяет изменять пароль пользователя JaCarta, пароль администратора JaCarta, пароль цифровой подписи, пароль разблокировки цифровой подписи. Описание параметров этой утилиты приведено в табл. 8.

Табл. 8

Параметры утилиты командной строки ase-pin-tool

Параметр	Описание
-l	Отображает список доступных считывателей.
-r	Позволяет задать активный считыватель.
-u	Позволяет изменить пароль пользователя. Допускаются только символы из набора ASCII. Если пароль пользователя заблокирован, сначала необходимо ввести пароль администратора.
-a	Позволяет задать пароль администратора JaCarta. Допускаются только символы из набора ASCII.
-d	Позволяет изменить пароль цифровой подписи. Допускаются только символы из набора ASCII. Если пароль цифровой подписи заблокирован, сначала необходимо ввести пароль разблокировки цифровой подписи.
-p	Позволяет изменить пароль разблокировки цифровой подписи. Допускаются только символы из набора ASCII.
-h	Отображает справку по использованию утилиты командной строки ase-pin-tool (на английском языке).

ПРИМЕР ИСПОЛЬЗОВАНИЯ

1. Подсоедините JaCarta к компьютеру.
2. Выполните следующую команду:

```
ase-pkcs-tool –u
```

Отобразится следующая строка:

```
Current User PIN:
```

3. Введите текущий пароль пользователя и нажмите клавишу ВВОД.
Отобразится строка для ввода нового пароля пользователя:

```
New User PIN:
```

4. Введите новый пароль пользователя и нажмите клавишу ВВОД.
Отобразится строка подтверждения нового пароля пользователя:

```
Confirm New User PIN:
```

5. Подтвердите новый пароль пользователя и нажмите клавишу ВВОД.
В случае успешной смены пароля пользователя отобразится следующее сообщение:

```
Program Succeeded
```

5. Настройка и использование JaCarta в Mozilla Firefox и Thunderbird

Для доступа к защищённому сайту с электронным ключом JaCarta можно использовать браузер Mozilla Firefox. Для этого необходимо выполнить следующие действия:

- подключить к Mozilla Firefox модуль PKCS#11 из состава установочного пакета;
- настроить Mozilla Firefox на использование JaCarta при установлении SSL- и TLS-соединений (требуется для Firefox 4.0 и более поздних версий).

Для шифрования, формирования и проверки подписи сообщений электронной почты с электронным ключом JaCarta можно использовать приложение Mozilla Thunderbird. Для этого необходимо подключить к Mozilla Thunderbird модуль PKCS#11.

5.1. Подключение модуля PKCS#11

Чтобы использовать электронные ключи JaCarta с браузером Mozilla Firefox или почтовым клиентом Mozilla Thunderbird по интерфейсу PKCS#11, в настройках соответствующего приложения укажите путь к файлу **libASEP11.so** из состава ПО.

Ниже рассматривается подключение модуля PKCS#11 к Mozilla Firefox. Подключение его к Mozilla Thunderbird осуществляется по аналогичной процедуре.

Для подключения модуля PKCS#11 к браузеру Mozilla Firefox выполните следующие действия.

1. В главном меню браузера Mozilla Firefox выберите **Правка > Настройки**.
2. В отобразившемся окне щёлкните на значке (раздел **Дополнительные**).
3. Выберите вкладку **Шифрование** и нажмите **Устройства защиты**.

Отобразится следующее окно.

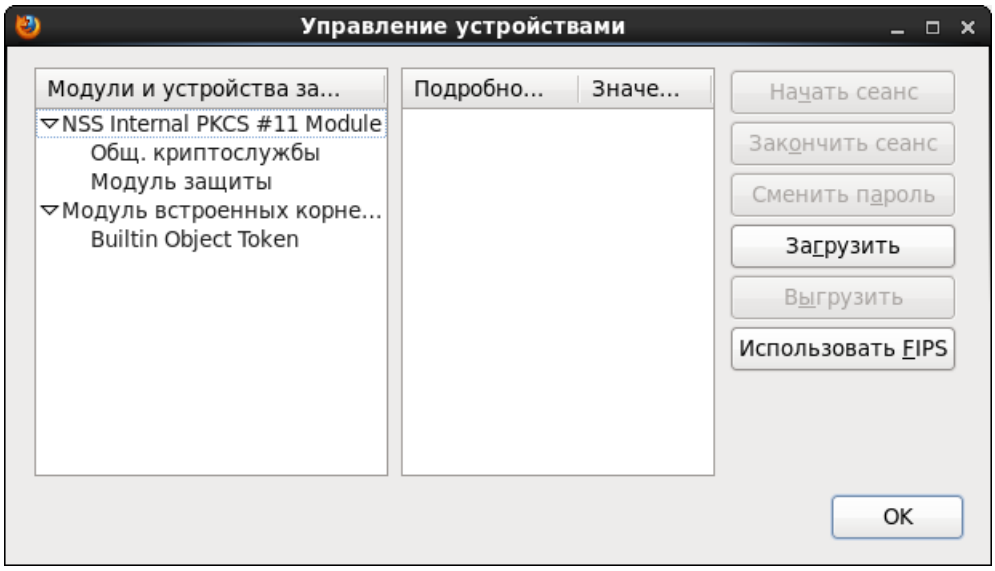

Рис. 14 – Окно **Управление устройствами**

4. Нажмите **Загрузить**.
   Отобразится следующее окно.

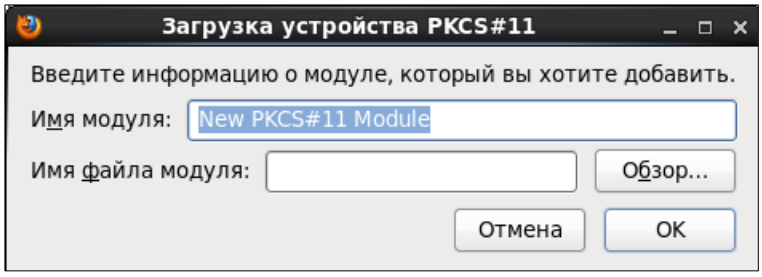

Рис. 15 – Окно **Загрузка устройства**

5. В поле **Имя модуля** задайте отображаемое имя (например, «JaCarta»).
6. В поле **Имя файла модуля** укажите путь к файлу libASEP11.so из состава ПО для использования JaCarta в среде Linux. При необходимости воспользуйтесь кнопкой **Обзор.**
7. Нажмите **ОК.**

Информация о подсоединённом электронном ключе JaCarta отобразится в окне управления устройствами.

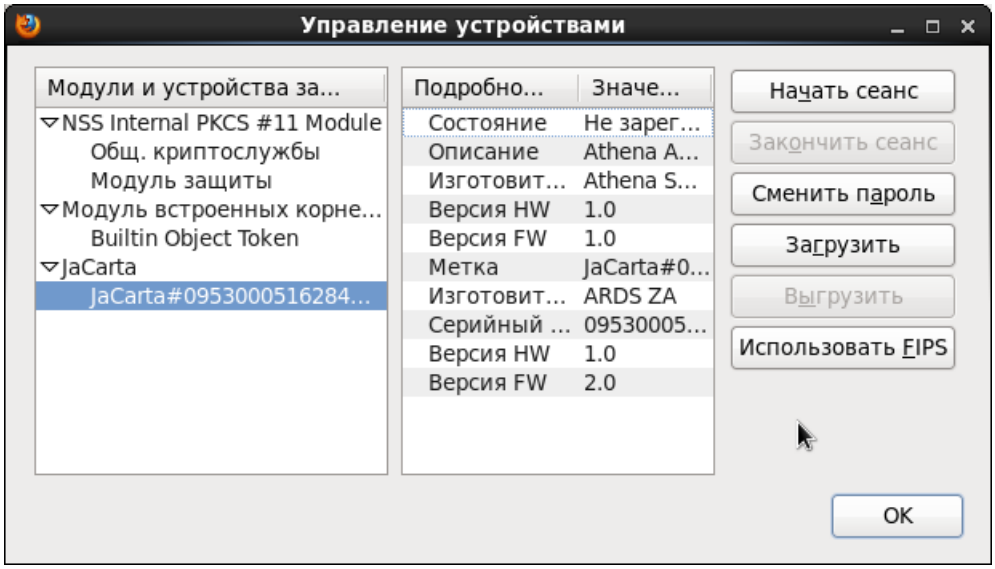

Рис. 16 – Информация о подсоединённом электронном ключе JaCarta в окне управления устройствами

Здесь также можно поменять пароль пользователя подсоединённого электронного ключа JaCarta, воспользовавшись кнопкой **Сменить пароль.**

8. Чтобы закрыть окно управления устройствами, нажмите **ОК.**

5.2. Настройка Mozilla Firefox для использования JaCarta при установлении SSL- и TLS-соединений

Чтобы обеспечить возможность доступа к защищённым сайтам по протоколам SSL и TLS с использованием закрытого ключа и цифрового сертификата в памяти JaCarta, выполните следующие действия.

Данные действия необязательны для Firefox версий до 4.0.

1. Запустите Mozilla Firefox.
2. В адресной строке наберите `about:config` и нажмите клавишу ВВОД.
   В окне браузера отобразится предупреждающее сообщение.
3. Щёлкните на кнопке **Я обещаю, что буду осторожен**.

Окно браузера примет следующий вид.

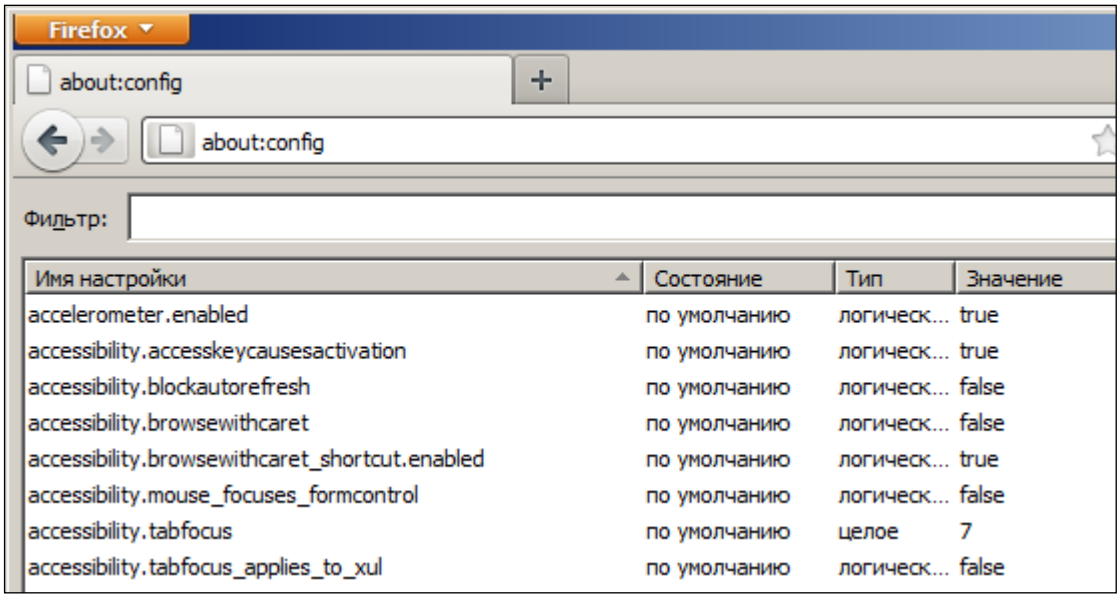

Рис. 17 – Список настроек Mozilla Firefox

4. Найдите настройку `security.ssl.allow_unrestricted_renego_everywhere__temporarily_available_pref` (для быстрого поиска настройки введите или скопируйте её имя в поле **Фильтр**).
5. Если она имеет значение **false** (ложь), двойным щелчком присвойте ей значение **true** (истина).

5.3. Пример использования

Чтобы получить доступ к защищённому сайту с использованием браузера Mozilla Firefox и электронного ключа JaCarta, выполните следующие действия.

1. Убедитесь в том, что к компьютеру подсоединён электронный ключ JaCarta.
2. Запустите браузер Mozilla Firefox.
3. В адресной строке введите адрес защищенного сайта (адрес должен начинаться с `https://`) и нажмите клавишу ВВОД.
   Отобразится следующее окно.

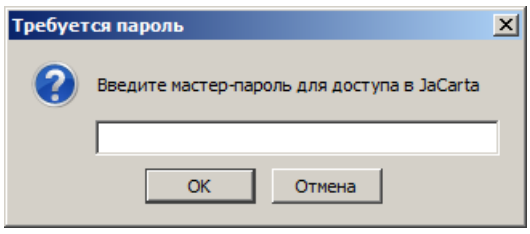

Рис. 18 – Окно ввода пароля пользователя электронного ключа JaCarta

4. Введите пароль пользователя электронного ключа JaCarta и нажмите **OK**.

Отобразится следующее окно.

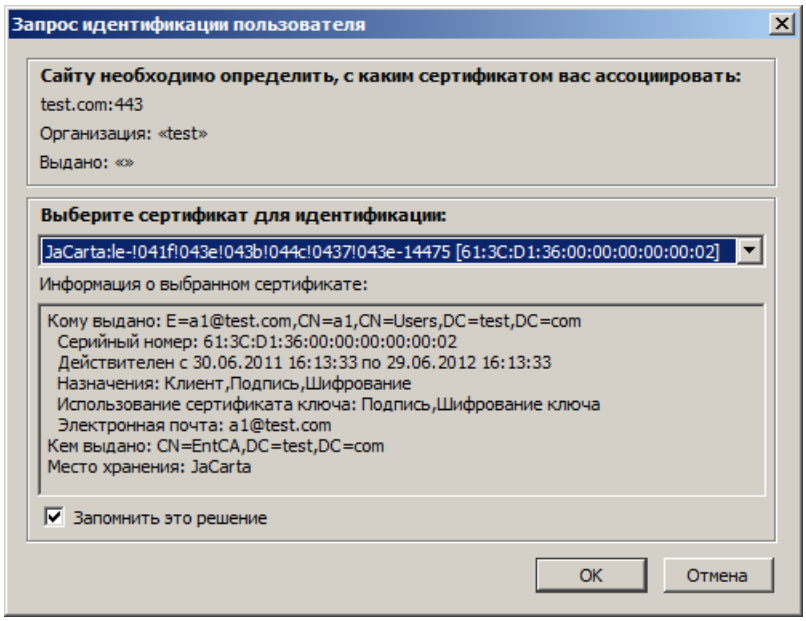

Рис. 19 – Окно идентификации пользователя

5. Установите флажок **Запомнить это решение** и нажмите **ОК**. Защищённая страница отобразится в окне браузера.

6. Список сокращений

ОС – операционная система

ПО – Программное обеспечение

SSL – Secure Socket Layer (Безопасный сокет и уровень)

TLS – Transport Layer Security (Протокол TLS)

PKCS – Public Key Cryptography Standards (Стандарты криптографии с открытым ключом)

PC/SC – Personal Computer/Smart Card (Персональный компьютер/смарт-карта), набор спецификаций для доступа к смарт-картам

ASCII – American Standard Code for Information Interchange (Американский стандартный код для обмена информацией)

CCID – Chip/Smart Card Interface Devices.

Лист регистрации изменений

Версия документа	Изменения
1.0	Исходная версия документа.
2.0	Добавлены сведение об установке на Astra Linux.

Телефон: +7 (495) 223-00-01
Факс: +7 (495) 646-64-40
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (бессрочно), № 2874 от 18.05.12
Лицензия ФСБ России № 12632 Н от 20.12.12
Microsoft Silver OEM Hardware Partner, Oracle Gold Partner, Apple Developer
Сертификат соответствия СМК ГОСТ Р ИСО 9001-2011