

АладдинРД

www.aladdin-rd.ru

Настройка аутентификации по смарт-картам eToken в XenDesktop 5.6 и XenApp 6.5 с тонких клиентов HP-t510 на базе ОС ThinPro

Краткое руководство

Версия 1.0

Аннотация

Настоящий документ содержит сведения о настройке аутентификации по смарт-картам в средствах доставки приложений XenApp версии 6.5 и рабочих столов XenDesktop версии 5.6.

По вопросам технической поддержки обращайтесь в ЗАО «Аладдин Р.Д.» по адресу: <http://www.aladdin-rd.ru/support/index.php>. Таким способом вы всегда сможете отслеживать состояние своей заявки.

Оглавление

Аннотация.....	1
Введение	3
Краткое описание инфраструктуры	3
Особенности тонких клиентов.....	4
Предварительная настройка тонкого клиента	4
Настройка даты и времени	4
Установка корневого сертификата УЦ.....	7
Настройка подключения к инфраструктуре Citrix	10
Добавление библиотеки в образ системы	10
Включение функции аутентификации по смарт-карте.....	12
Настройка Web-браузера.....	13
Проверка корректности настройки	19
История изменений.....	23

Введение

Краткое описание инфраструктуры

- Microsoft Windows Server 2008 R2 - Контроллер домена (DC.aladdin.local)
- Microsoft Windows Server 2008 R2 – Центр сертификации MSCA (CA.aladdin.local)
 - SAC 8.2
- Microsoft Windows Server 2008 R2 – XenDesktopServer (XD.aladdin.local)
 - XenDesktop 5.6
- Microsoft Windows Server 2008 R2 – XenAppServer (XA.aladdin.local)
 - XenApp 6.5
- Microsoft Windows Server 2008 R2 – Web-интерфейс (WI.aladdin.local)
- HP-t510 ThinPro 4.4.0 – Тонкий клиент
- Microsoft Windows 7 32-bit – Тестовая эталонная машина (win71.aladdin.local)
 - Citrix Receiver 3.4.
 - SAC_Post_GA 8.2.116
 - Virtual Delivery Agent

Особенности тонких клиентов

В настоящее время такое решение, как тонкий клиент получило огромную популярность. Многие модели тонких клиентов оснащены интерфейсами для подключения к серверам виртуализации Citrix, VmWare, Microsoft TS и т.д. Основная проблема по настройке аутентификации по смарт-картам к виртуальным инфраструктурам возникает из-за того, что на многие тонкие клиенты, как правило, не устанавливаются операционные системы или устанавливаются урезанные Linux-подобные системы. В связи с этим на подобные тонкие клиенты становится проблематичным установка драйверов и дополнительного программного обеспечения.

Линейка устройств eToken, кроме eToken PRO 32/64K, являются CCID-совместимыми устройствами и для их определения в Linux системах достаточно установленного пакета pcsc и информации об устройстве в файле Info.plist (VID, PID, Название устройства). Как правило, этот компонент уже включен в образы Linux-подобных систем большинства производителей тонких клиентов, но не все интерфейсы подключения умеют взаимодействовать с устройствами.

В данном документе будет описан способ настройки аутентификации по смарт-картам eToken в инфраструктуре Citrix XenApp 6.5 и Citrix XenDesktop 5.6 с тонких клиентов Hewlett-Packard HP-t510 на базе Linux-подобной операционной системы ThinPro 4.4.0

Предварительная настройка тонкого клиента

Настройка даты и времени

Для того, чтобы стало возможным настраивать тонкий клиент, необходимо перейти в режим администрирования (см. изображение ниже).



Рис. 1 – Переход в режим администрирования

Далее, необходимо убедиться, что установлена актуальная версия операционной системы. В нашем случае это ThinPro версии 4.4.0.

Внимание:

Для возможности проверки и скачивания обновлений с ресурсов HP, необходимо чтобы тонкий клиент имел выход в Internet.

Для того, чтобы проверить версию операционной системы (ОС) тонкого клиента, необходимо запустить **Easy Config Wizard** и перейти к пункту **Updates** (см. изображение ниже).

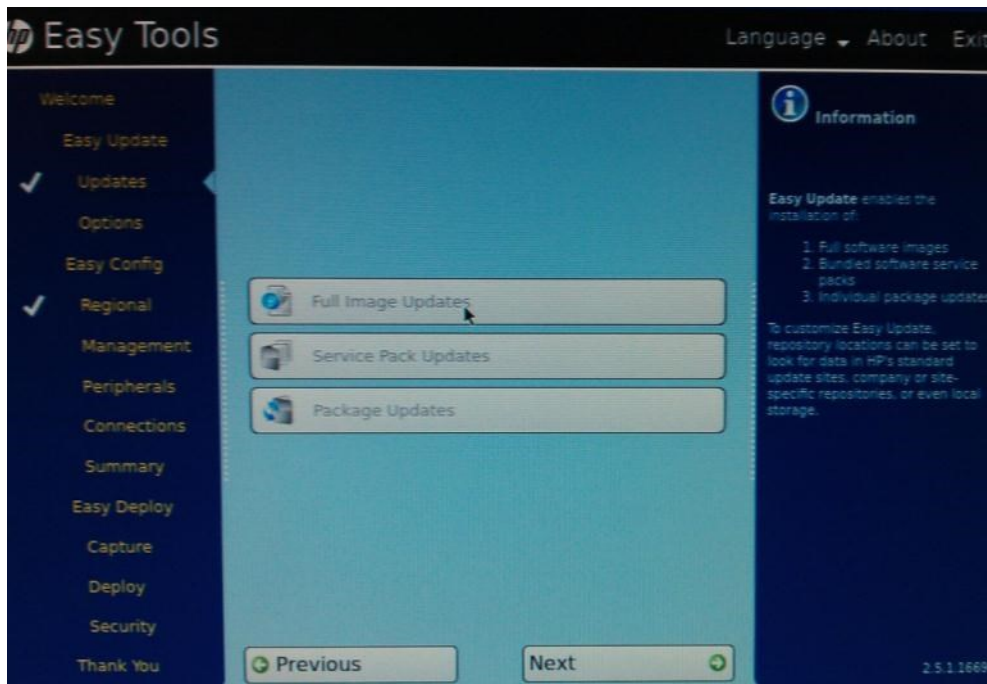


Рис. 2 – Easy Config Wizard

Нажимаем **Full Image Updates**

В открывшемся окне видно какая операционная система в данный момент установлена на тонком клиенте. В нашем случае это **ThinPro 4.4.0**.

Если у Вас установлена более старая версия ОС, выберете версию **ThinPro 4.4.0** и нажмите **Install** (см. изображение ниже).

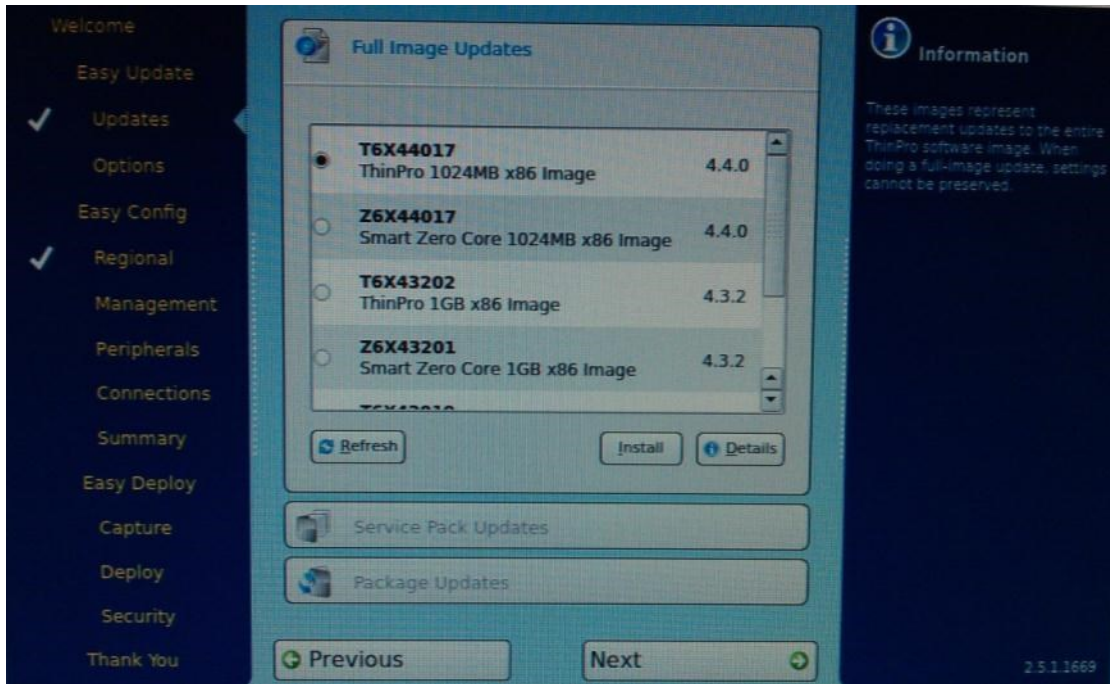


Рис. 3 – Образ ОС

Убедившись, что установлена актуальная версия ОС, переходим к настройке даты и времени. Это необходимо сделать для того, чтобы не было проблем с установкой SSL соединения между клиентом и сервером.

Чтобы установить время перейдите в **Control Panel** и откройте вкладку **Setup** (рис. 4).



Рис. 4 – Control Panel (Setup)

Открываем **Date and Time**

Появится следующее окно, в котором необходимо настроить местоположение и часовой пояс.

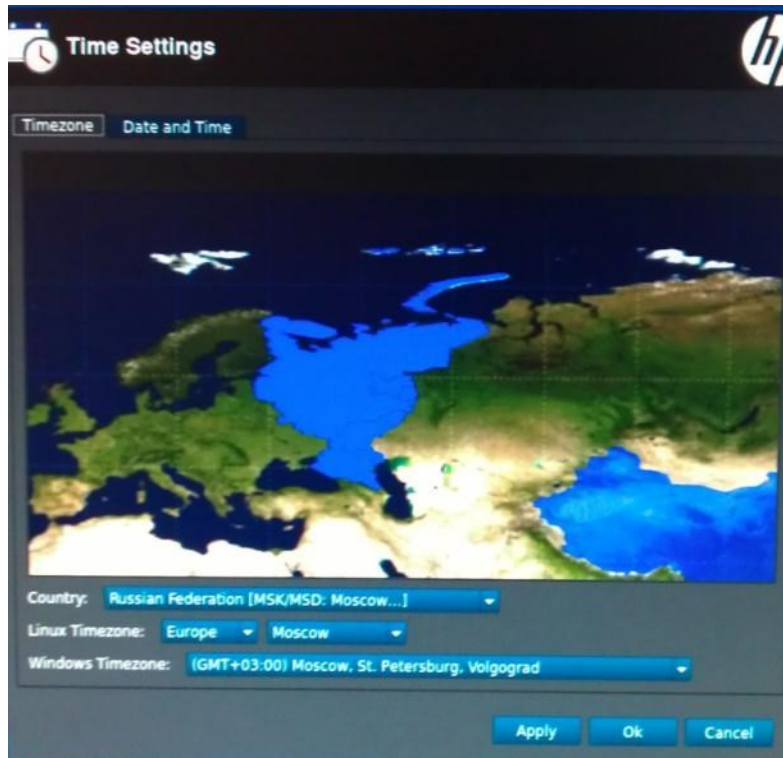


Рис. 5 – Часовой пояс

Переходим на вкладку **Date and Time**, где необходимо установить дату и время, аналогичную дате и времени установленной на удаленном сервере Citrix.

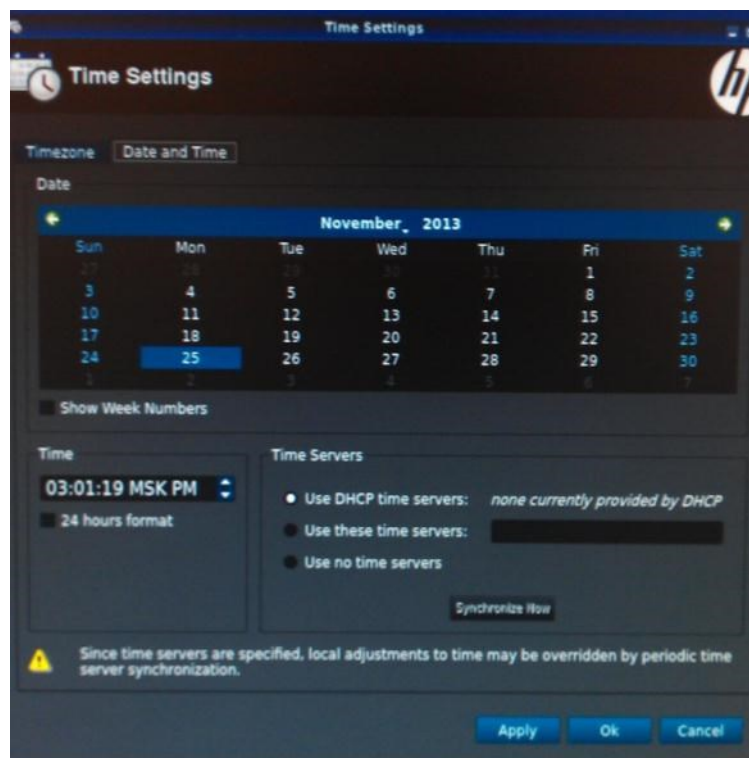


Рис. 6 – Дата и время

Установка корневого сертификата УЦ

Для установки SSL-соединения между тонким клиентом и сервером необходимо на тонкий клиент установить сертификат корневого центра сертификации. Копируем корневой сертификат УЦ на съемный носитель (USB-Flash) и подключаем его к тонкому клиенту. Открываем **Control Panel** и переходим на вкладку **Advanced**. Выбираем **Certificates** (рис. 7)



Рис. 7 – Advanced (Certificates)

Открывается следующее окно (рис. 8)



Рис. 8 – Certificates

Нажимаем **Import From File**

Находим сертификат корневого УЦ на съемный носитель и импортируем его. Появится окно, показывающее, что сертификат успешно импортирован (см. изображение ниже)

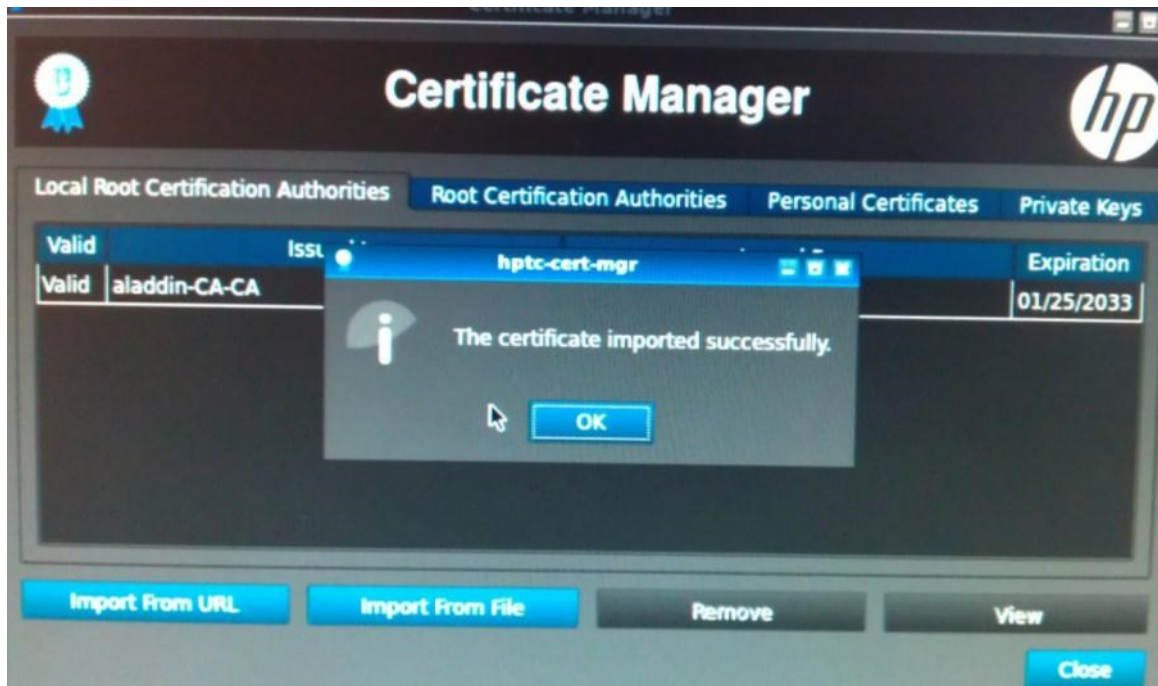


Рис. 9 – Imported successfully

На этом предварительная настройка тонкого клиента завершается.

Настройка подключения к инфраструктуре Citrix

Добавление библиотеки в образ системы

Для того, чтобы Citrix ICA Client мог работать с устройства eToken, для начала необходимо добавить PKCS#11 библиотеку в образ системы.

Копируем библиотеку libeToken.so на съемный носитель (USB-Flash)

Внимание:

Библиотека libeToken.so входит в состав установочного пакета SAC для Linux

Подключаем съемный носитель к тонкому клиенту, открываем **Control Panel** и переходим на вкладку **Advanced**



Рис. 10 – Advanced (X Terminal)

Запускаем **X Terminal**

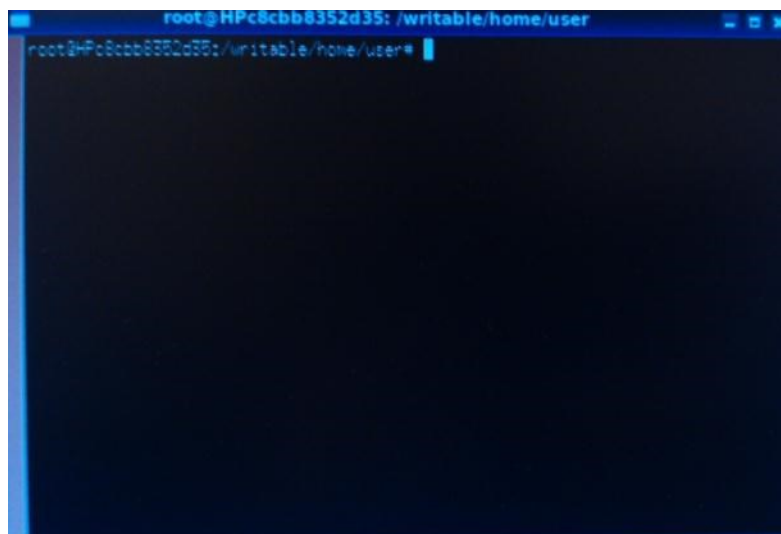
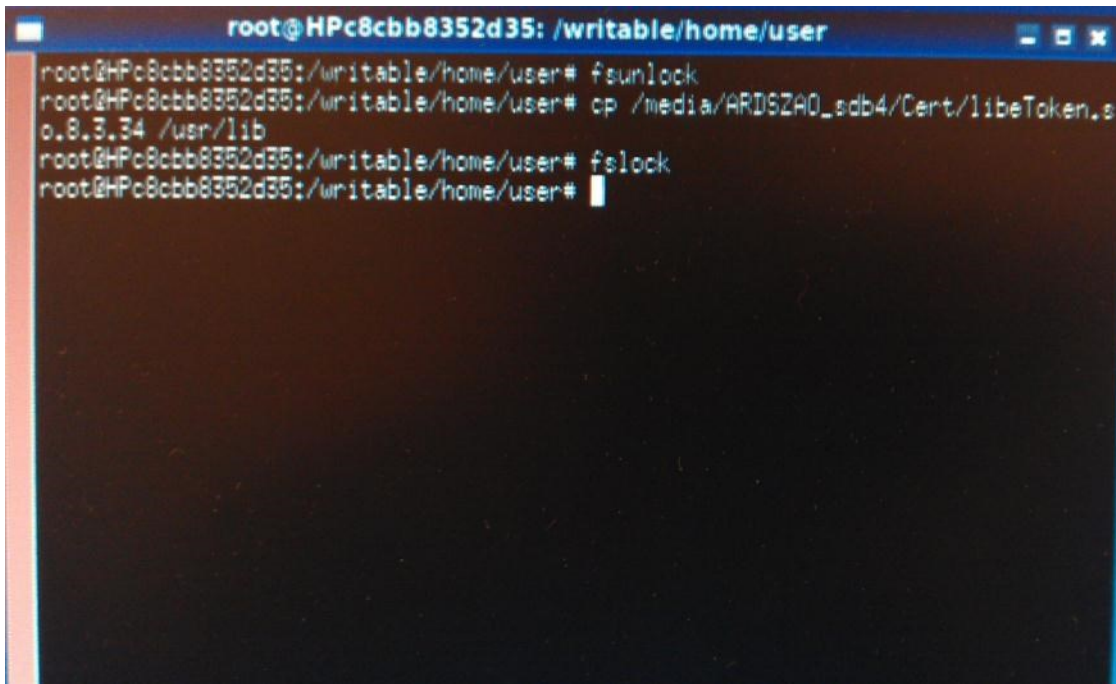


Рис. 11 – X Terminal

Разблокируем файловую систему для получения возможности изменения и добавления файлов командой **fsunlock**.

Копируем файл **libeToken.so** в каталог **/usr/lib** командой **cp /путь к каталогу на съемном носителе/libeToken.so /usr/lib**

После этого выполняем команду **fslock** для того, чтобы заблокировать возможность изменения файлов системы (см. изображение ниже).



```
root@HPc8cbb8352d35: /writable/home/user
root@HPc8cbb8352d35:/writable/home/user# fsunlock
root@HPc8cbb8352d35:/writable/home/user# cp /media/ARDISZA0_sdb4/Cert/libeToken.so.8.3.34 /usr/lib
root@HPc8cbb8352d35:/writable/home/user# fslock
root@HPc8cbb8352d35:/writable/home/user#
```

Рис. 12 –Копирование библиотеки

Закрываем окно **X Terminal**

Включение функции аутентификации по смарт-карте

В главном окне выбираем **Connections**, раскрываем вкладку **General Settings** и открываем **Citrix**

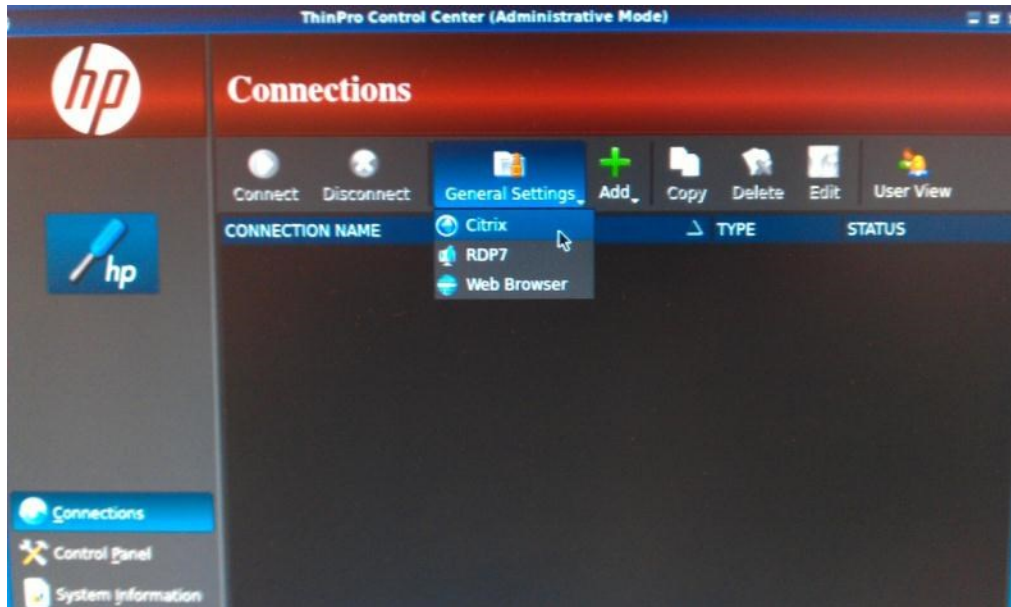


Рис. 13 –General Settings (Citrix)

Откроется окно настроек **Citrix Connection**,
Здесь необходимо установить галочку напротив **Allow Smart Card Logon** – разрешить вход по смарт-карте



Рис. 14 – Citrix connection settings

Принимаем изменения и закрываем окно

Настройка Web-браузера

Внимание:

С данного тонкого клиента подключение по смарт-картам к инфраструктуре Citrix поддерживается только через Web-интерфейс

Раскрываем вкладку **General Settings** и открываем **Web Browser**



Рис. 15 – General Settings (Web Browser)

Откроется окно настройки **Web-браузера**

Здесь необходимо установить галочку напротив **Allow connections to manage their own settings**, для того, чтобы появилась возможность управления настройками **Web-браузера**. (рис. 16)

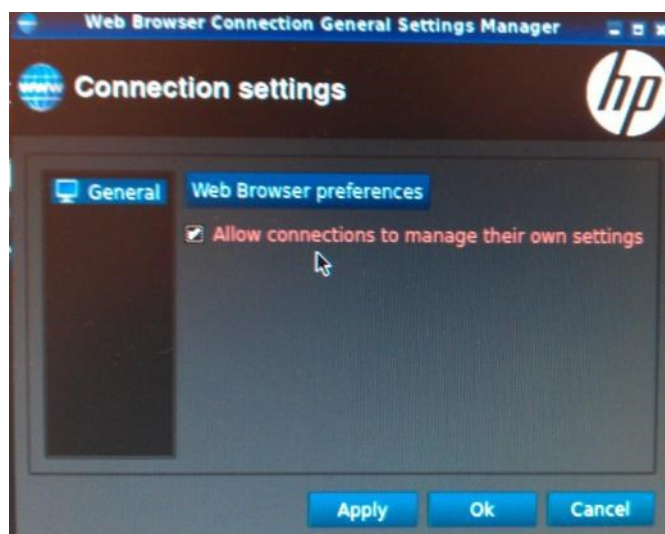


Рис. 16 – Окно настройки браузера

Нажимаем **Ok**.

Теперь добавим новое подключение.

Раскрываем вкладку **Add** и нажимаем **Web Browser**

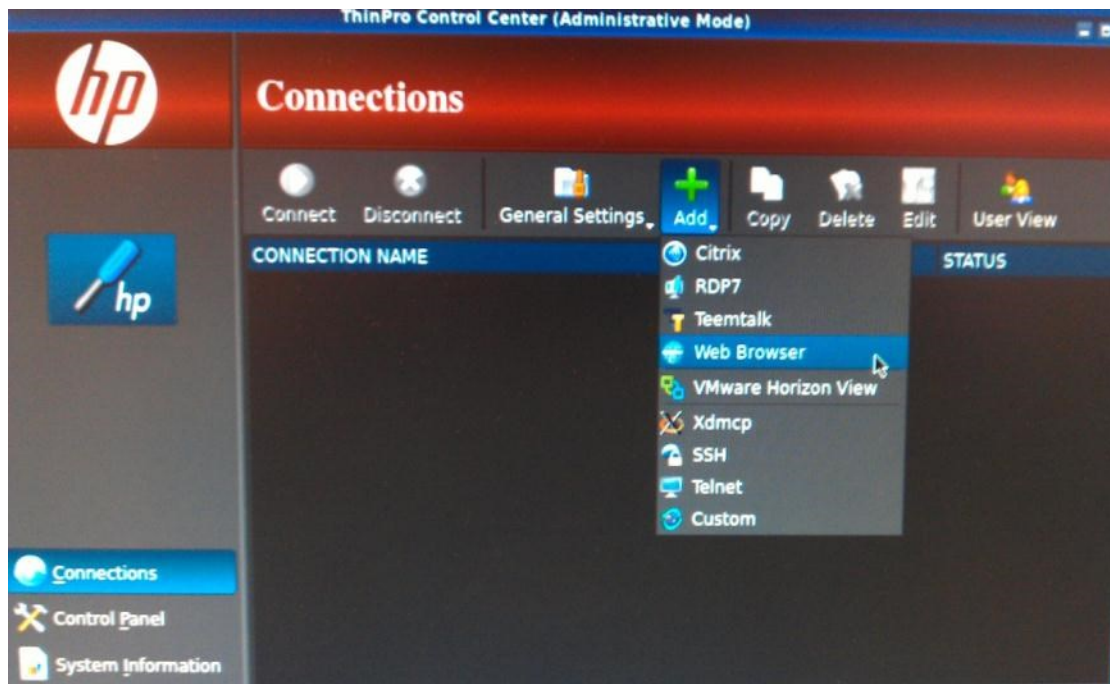


Рис. 17 – Add (Web Browser)

Откроется следующее окно, в котором необходимо заполнить поля: имя подключения **Name** и **URL** для подключения к Web-интерфейсу Citrix (см. изображение ниже)

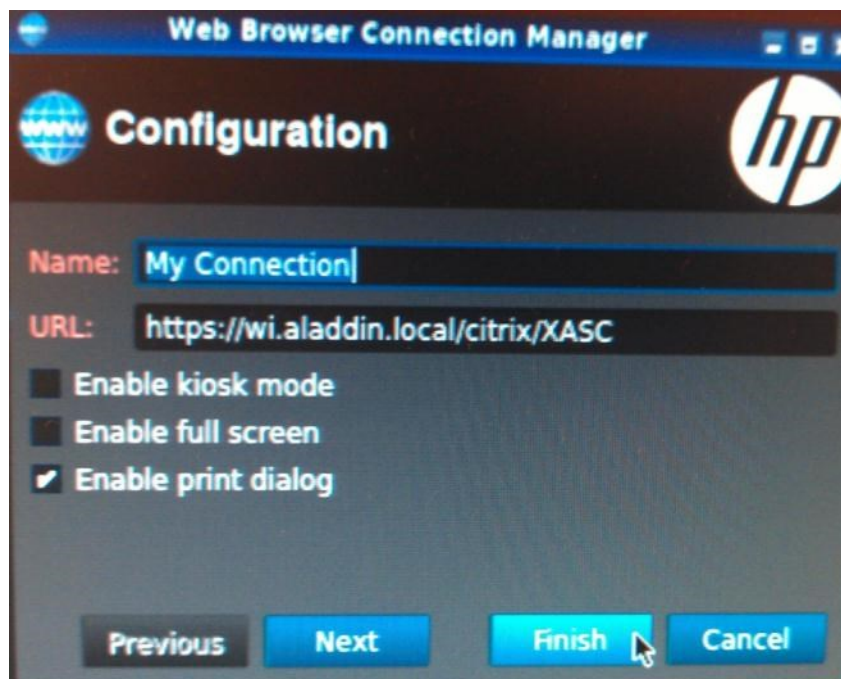


Рис. 18 –Web Browser (New connection)

Нажимаем **Finish**

Видим, что подключение **My Connection** успешно добавлено.

Запускаем созданное подключение

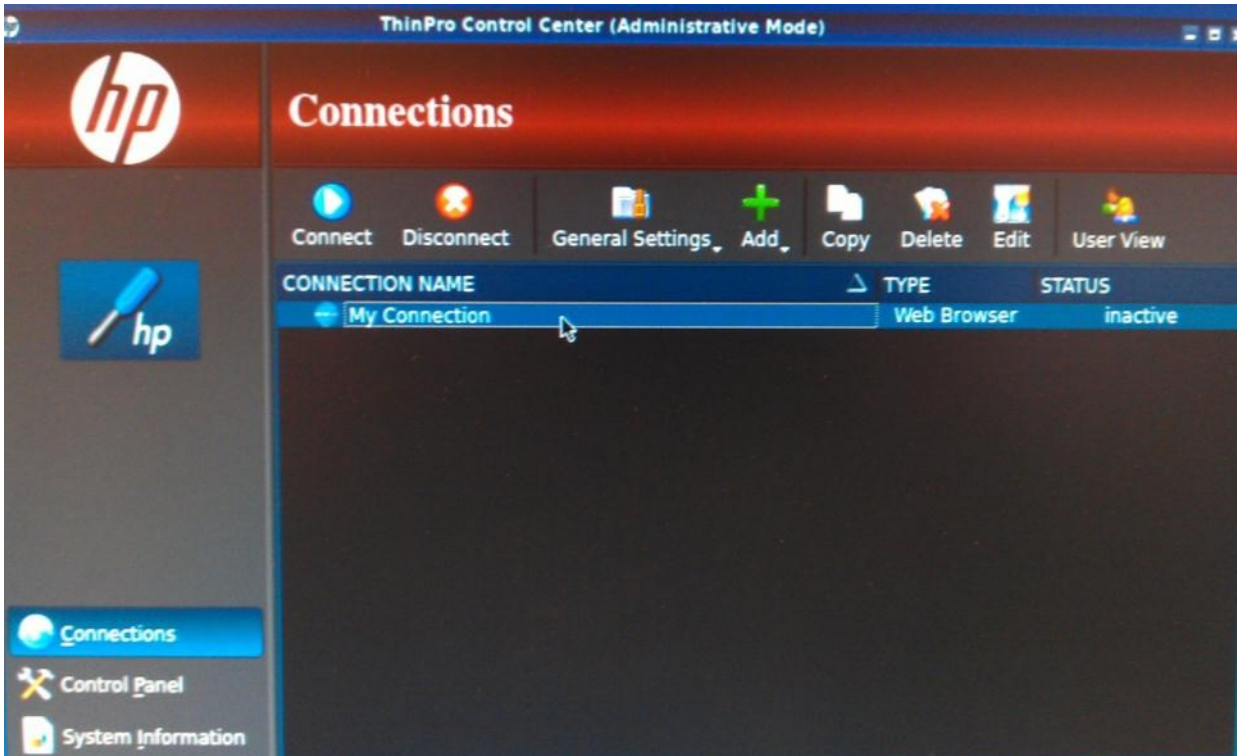


Рис. 19 –My Connection

Открывается браузер, в котором необходимо добавить поддержку устройства eToken, для этого нажимаем **Edit** -> **Preferences** (см. изображение ниже).

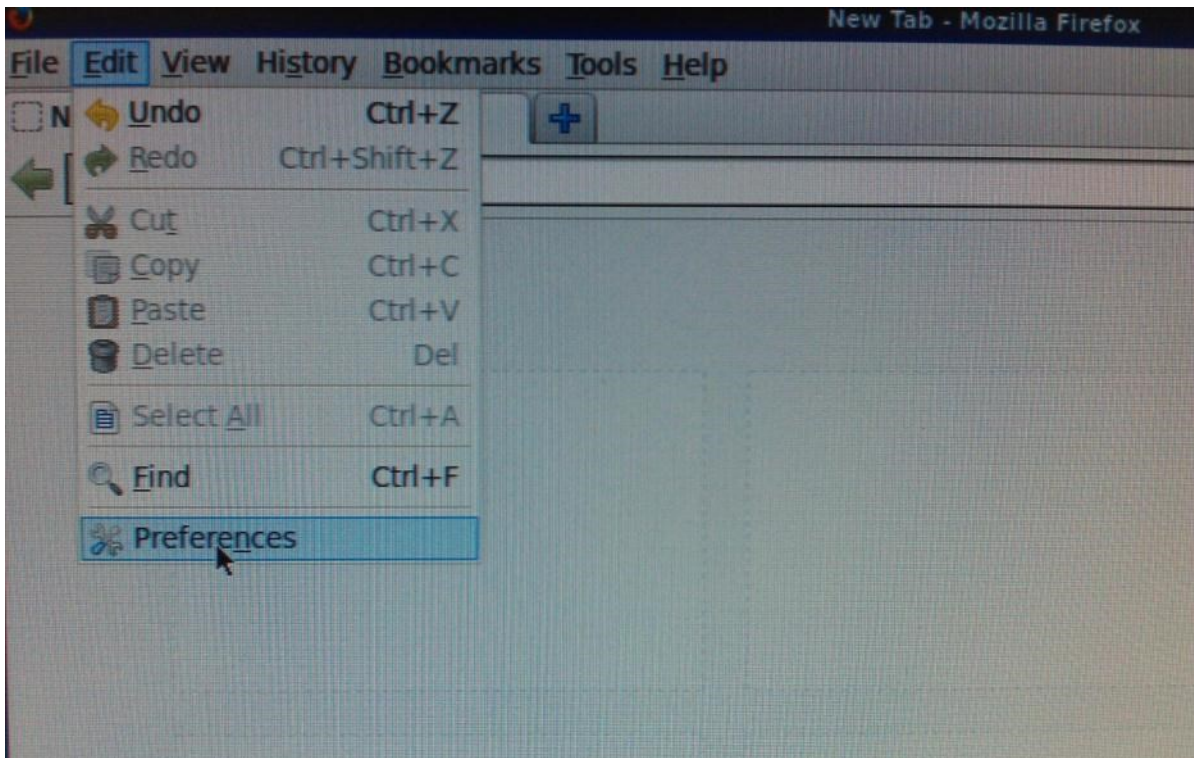


Рис. 20 – Firefox (Preferences)

Переходим на вкладку **Advanced** -> **Certificates** и открываем **Security Devices**

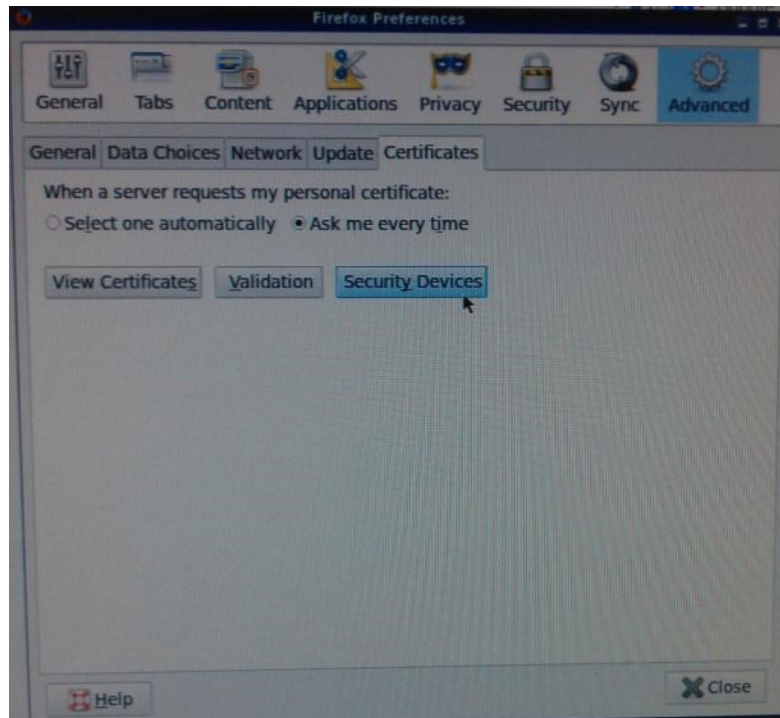


Рис. 21 – Firefox (Security Devices)

Для добавления устройства в открывшемся окне нажимаем **Load** (рис. 22)

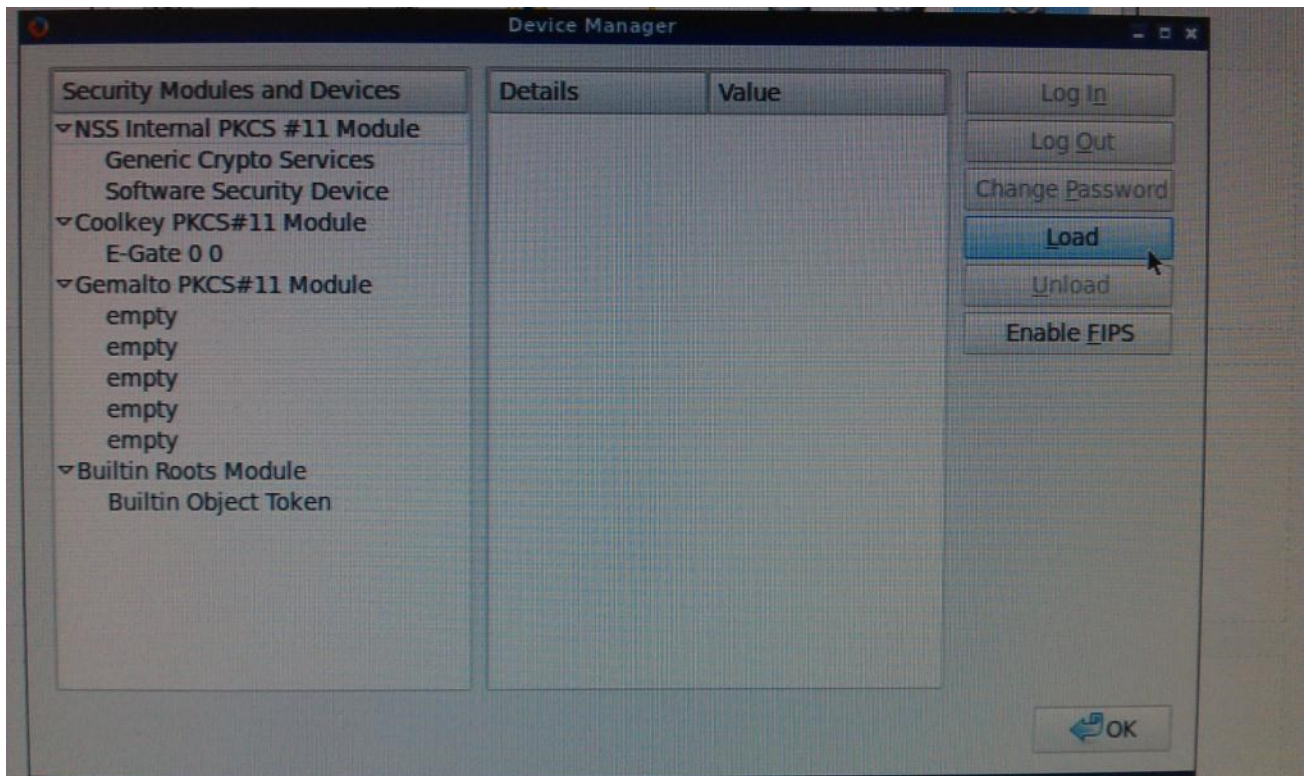


Рис. 22 – Firefox (Device Manager)

Выбираем скопированную ранее библиотеку **libeToken.so** и нажимаем **Open**

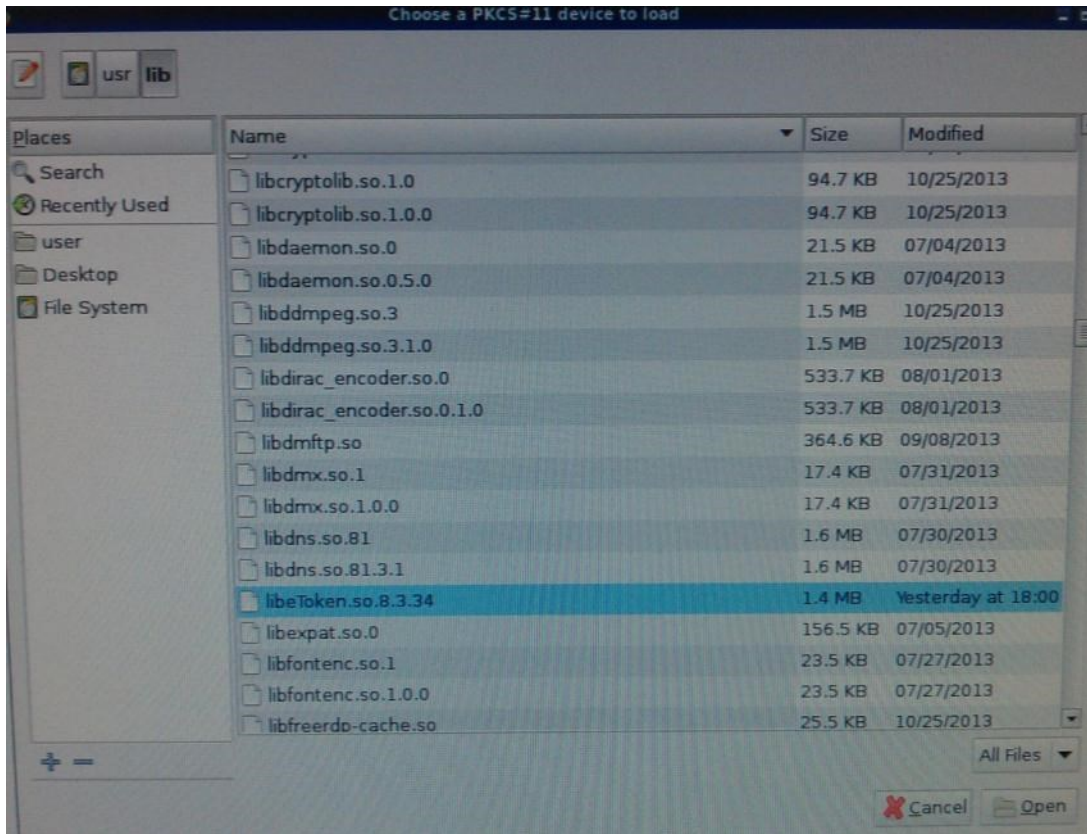


Рис. 23 – Firefox (Choose PKCS#11)

Проверяем правильность добавляемой информации (см. изображение ниже)

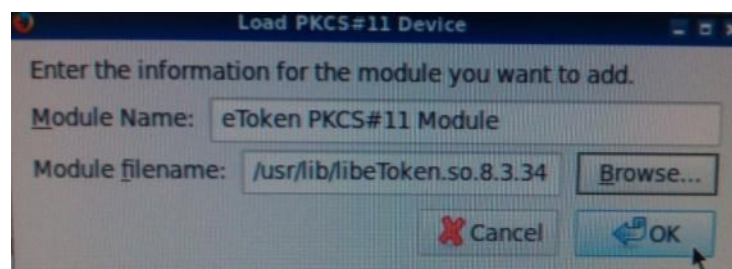


Рис. 24 – Firefox (Load PKCS#11)

Нажимаем **OK**

Устройство успешно добавлено.

Если подключить **eToken**, появляется запись о подключенном устройстве и информация о нем. (см. рисунок 25)

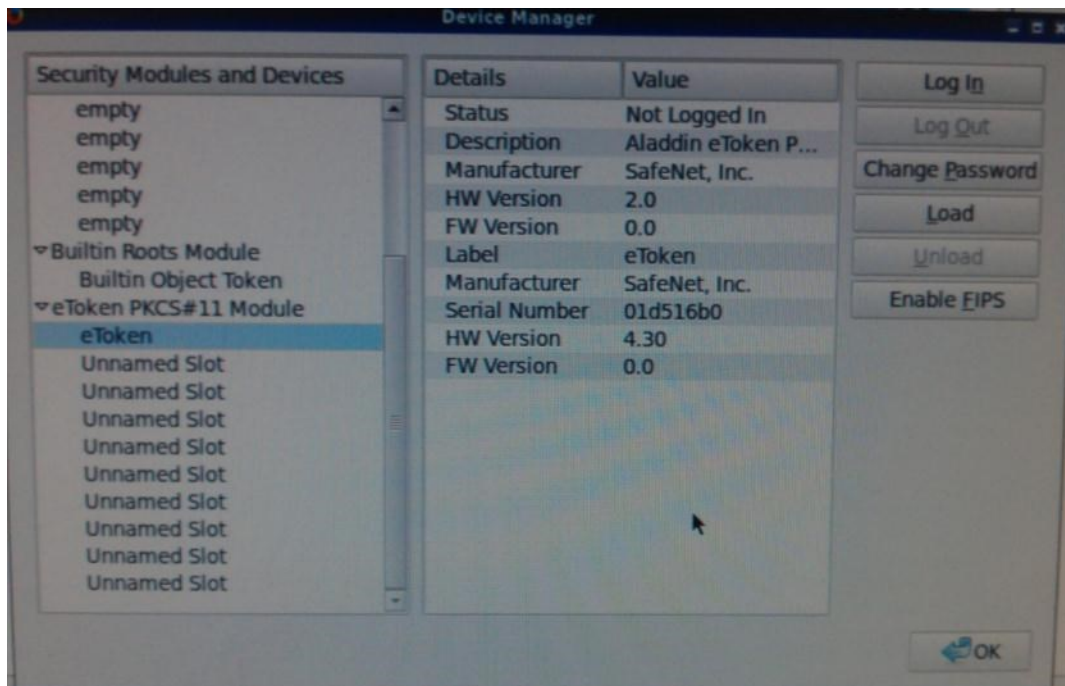


Рис. 25 – Firefox (eToken PKCS#11 Module)

Нажимаем **OK** и закрываем браузер.

На этом настройка аутентификации по смарт-картам завершается. Переходим к проверке работоспособности.

Проверка корректности настройки

Запускаем созданное ранее подключение.

В случае если отобразится следующее окно (см. изображение ниже)

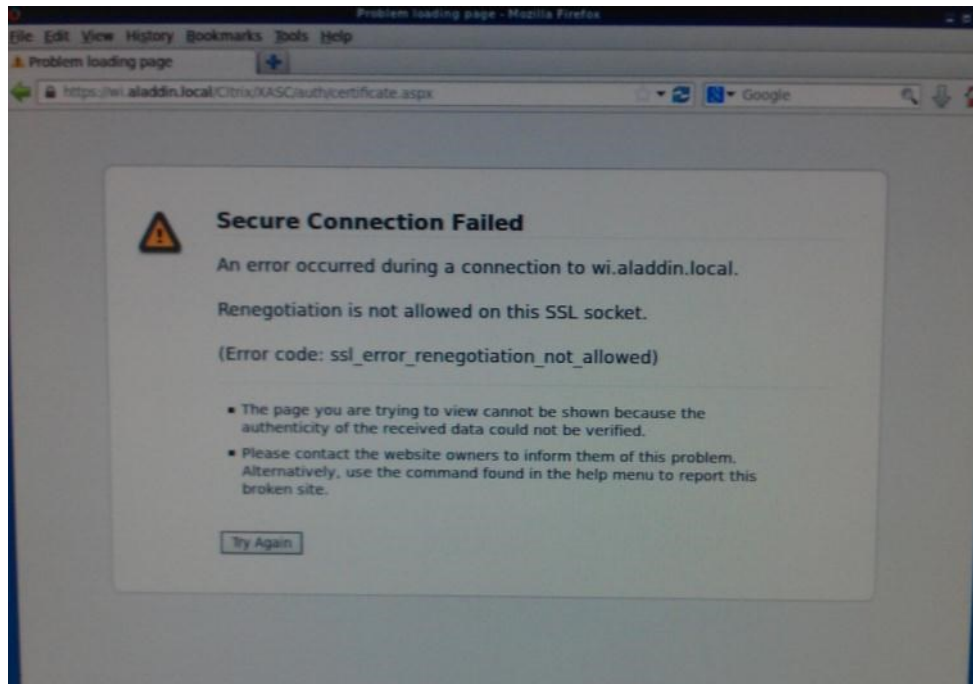


Рис. 26 – Firefox (Secure Connection Failed)

заходим в расширенные настройки браузера, для этого необходимо в адресной строке написать about:config

В поиске ищем **security.ssl.allow_unrestricted_renego_every...** и меняем значение на **true** (см. изображение ниже)

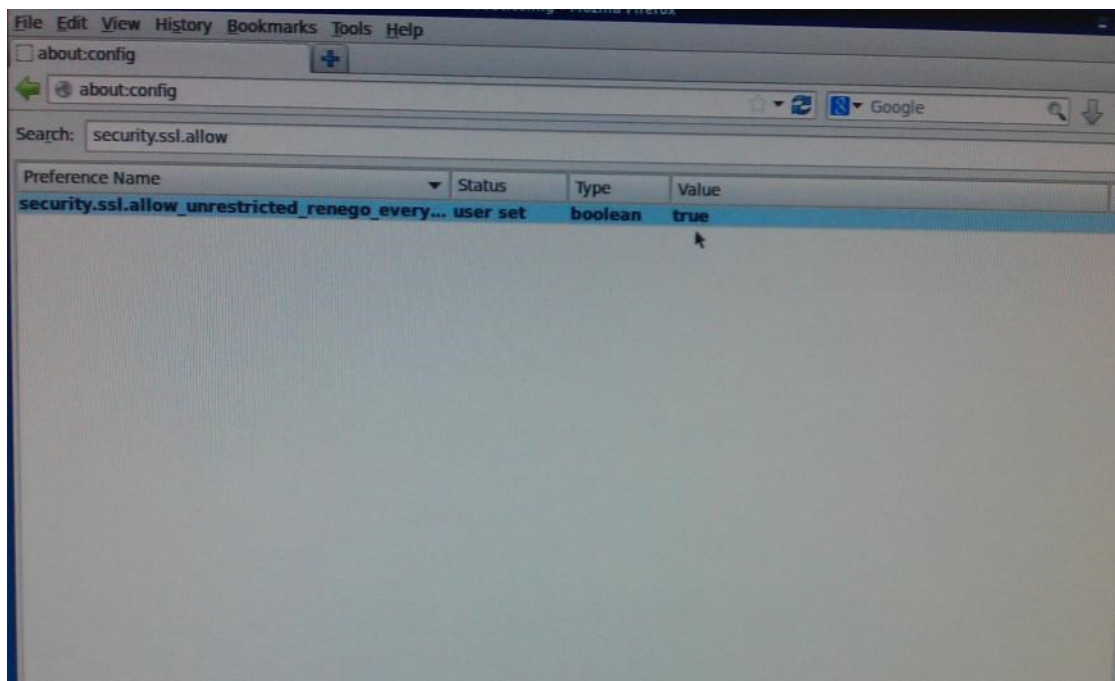


Рис. 27 – Firefox (Secure SSL Allow)

Закрываем браузер и снова открываем созданное подключение **My Connection**

Если все настроено правильно и устройство eToken подключено к терминальному клиенту, то при подключении к Web-интерфейсу, браузер запросит пин-код.

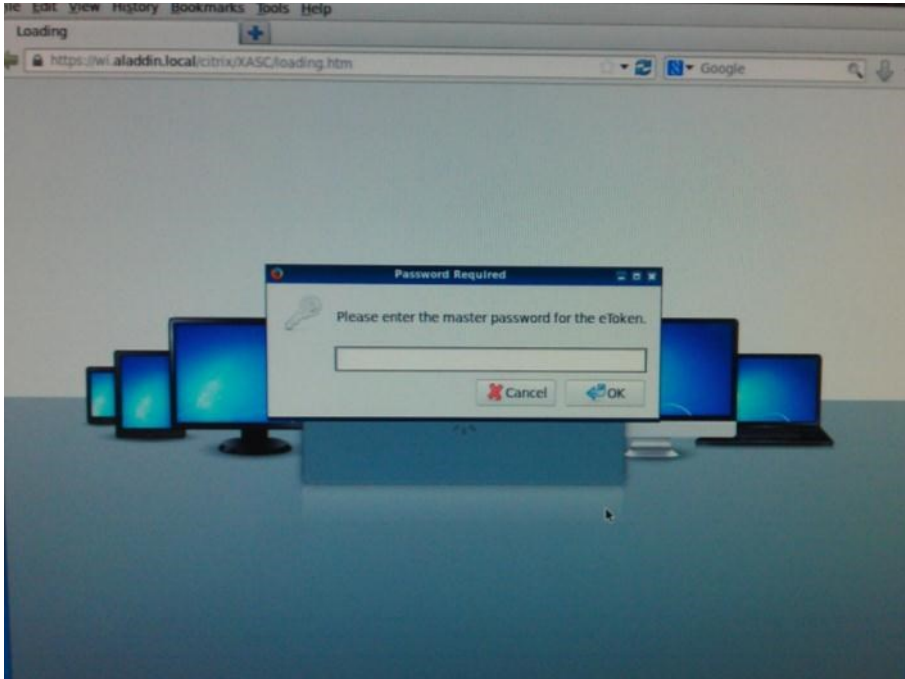


Рис. 28 – Запрос пин-кода браузером

Вводим пин-код и нажимаем **ОК**.

Выбираем сертификат с использованием которого будет осуществлен вход в Web-интерфейс

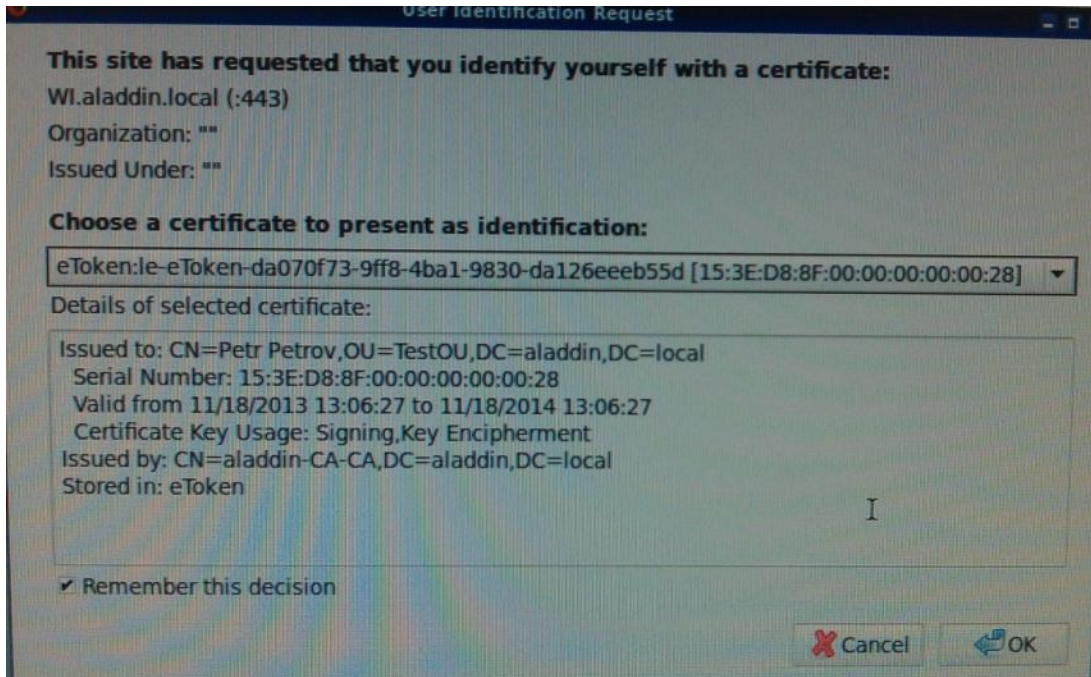


Рис. 29 – Выбор сертификата для входа

Нажимаем **ОК**

Открывается окно с доступными пользователю программами и рабочими столами.

Выбираем приложение (рабочий стол) к которому требуется подключиться.

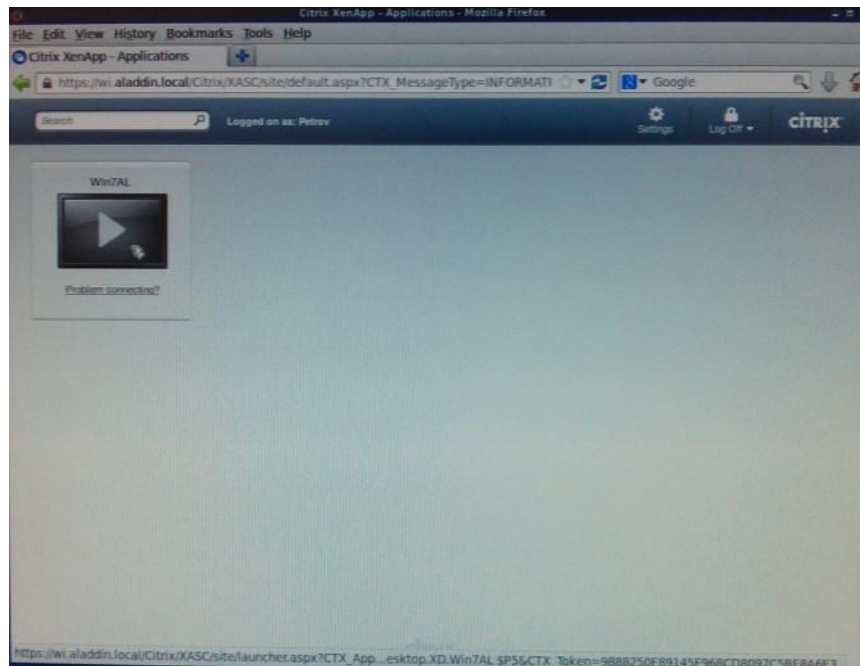


Рис. 30 – Доступные приложения и рабочие столы

Запускаем приложение (рабочий стол). В данном документе в качестве примера мы подключаемся к виртуальному рабочему столу Windows 7 32-bit.

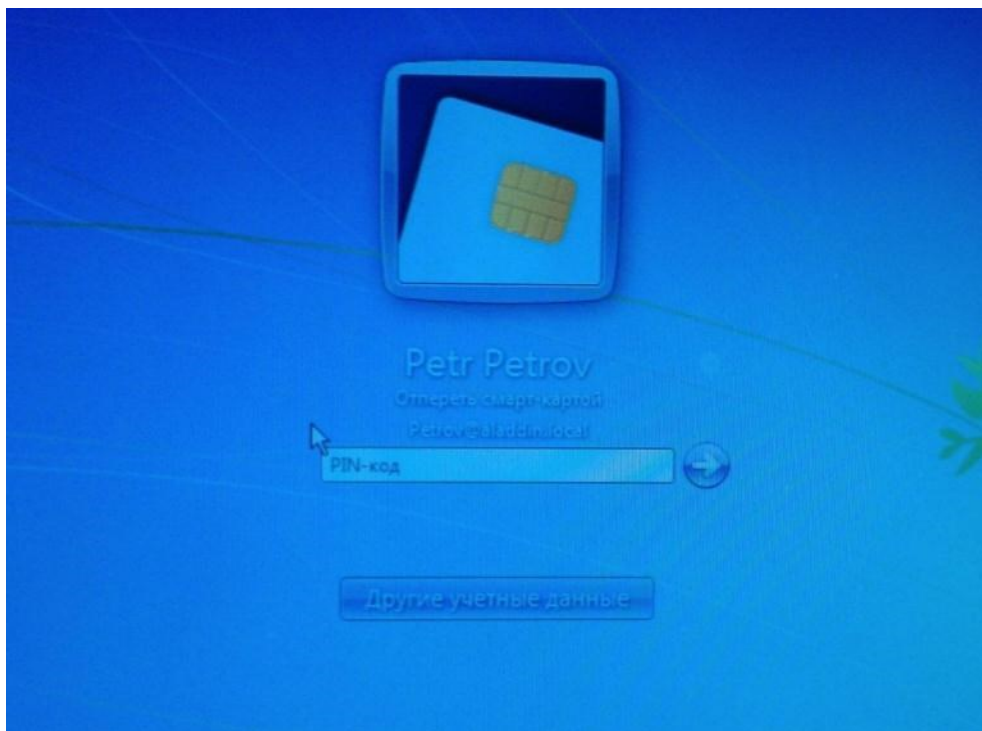


Рис. 31 – Запрос пин-кода на удаленной машине

Вводим **пин-код** пользователя.

Аутентификация на удаленной машине прошла успешно.

Запустив **SafeNet Authentication Client Tools** можно убедиться, что устройство корректно пробро- силось в сессию (см. изображение ниже)

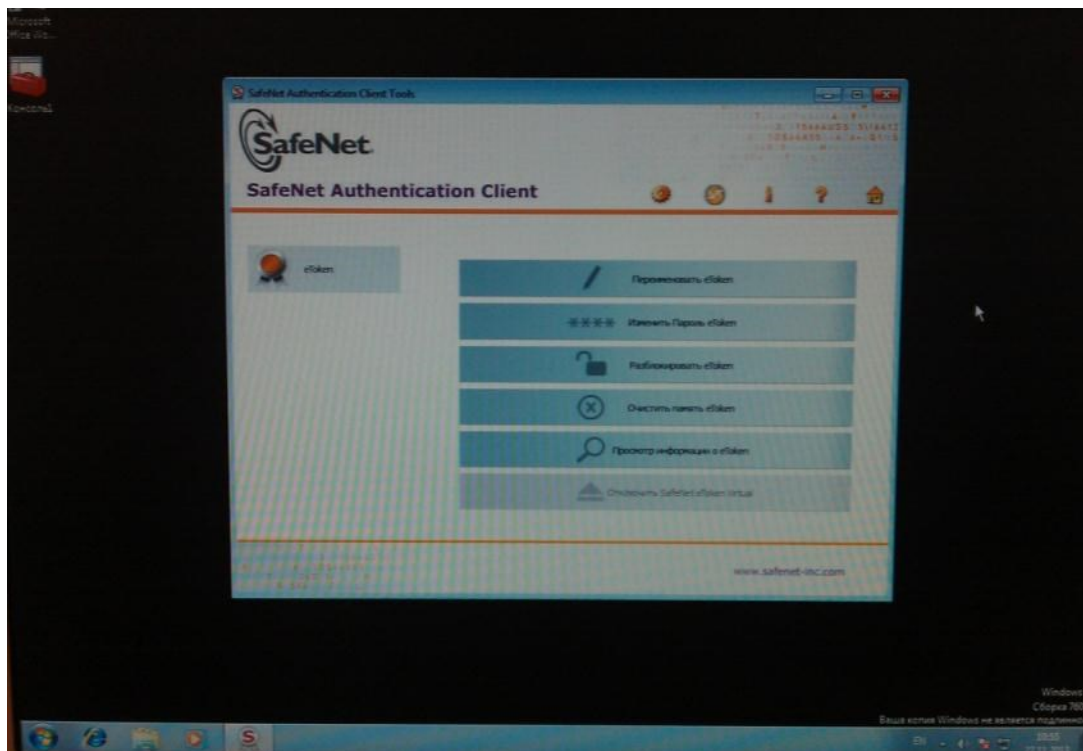


Рис. 32 – SAC Tools

История изменений

Версия	Описание изменений
1.0	Исходная версия документа.

Аладдин 

© 1995-2013, ЗАО "Аладдин Р.Д."
Все права защищены

+7 (495) 223-00-01;

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12 и № 18229 от 13.10.10

Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2008
Сертификат СМК ГОСТ Р ИСО 9001-2008 № РОСС RU.ИС72.К00069 от 16.07.12
Microsoft Silver OEM Hardware Partner, Apple Developer

aladdin@aladdin-rd.ru;

www.aladdin-rd.ru

Microsoft Partner
Silver OEM Hardware

 **Developer**

