Аутентификация в OpenSSH Putty по JaCarta PKI

Руководство по настройке

Версия продукта:	1.0
Версия документа:	1.0
Редакция от:	6 июля 2016 г.
Статус:	Внутренний документ
Листов:	12
Автор:	Т. Алексеев

Аннотация

Документ описывает алгоритм настройки SSH-клиента Putty для ОС Windows для работы с JaCarta PKI.

Оглавление

Общия сведения

SSH

SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH поддерживает возможность аутентификации по rsa ключу, что обеспечивает максимальный уровень безопасности для канала передачи данных, а также двухфакторную аутентификацию удаленных пользователей.

Аутентификация по сертификату

Для настройки работы SSH по RSA сертификатам необходимо настроить SSH сервер, а также SSH клиента на клиентской машине. В данном документе описан алгоритм настройки работы SSH с использованием смарт-карты либо токена JaCarta PKI, для целей аутентификации и шифрования установленного канала.

Настройка смарт-карт для SSH-клиента

Порядок настройки серверной части на примере Ubuntu

Генерация ключевой пары утилитой ssh-keygen.

i. Переходим в директорию /home/user/.ssh

ii. `ssh-keygen -t rsa`

iii. Задать имя ключа, например key

iv. Задать пароль ключа (для шифрования закрытого ключа) например 12345678

v. На выходе получаем два файла например key и key.pub

Генерация запроса на сертификат с ключами из п.1

vi. `openssl req -new -out user.req -key key`

Выпуск сертификата в CA openssl

vii. Настройка openssl CA

1. `cd /etc/ssl`
2. `sudo -i`

3. `echo "01" > serial`
4. `cp /dev/null index.txt`
5. редактируем /etc/ssl/openssl.cnf `nano openssl.cnf`
    a. `dir = ./`
    b. `certs = $dir/certs`
    c. `crl_dir = $dir/crl`
    d. `database = $dir/index.txt`
    e. `new_certs_dir = $dir/certs`
    f. `certificate = $dir/ca.crt`
    g. `serial = $dir/serial`
    h. `crl = $dir/crl.pem`
    i. `private_key = $dir/ca.key`
6. `openssl req -new -x509 -keyout ca.key -out ca.crt -days 3650`
7. `mkdir crl`
8. Скачать https://yadi.sk/d/zScNa_7CtHTdL make_hash_link.sh
9. Запуск makehashlink
10. `chmod +x make_hash_link.sh`
11. `./make_hash_link.sh /etc/ssl`
12. `./make_hash_link.sh /etc/ssl/crl`

viii. Подписание сертификата пользователя (выпуск)

1. `sudo -i`
2. `cd /home/user/.ssh`
3. `openssl ca -out user.crt -infiles user.req`

Импорт открытого ключа в Autorized_keys

ix. В директории `/home/user/.ssh` должен находиться файл открытого ключа, содержащий `ssh-rsa {KEY}`. В примере мы создали файл с именем `key.pub`

x. Импортируем данный ключ в файл authorized_keys

xi. `echo key.pub > authorized_keys`

Донастройка серверной части

b. `chmod 700 authorized_keys`

c. Настройки openssh. В /etc/ssh/sshd.conf редактируем конфигурацию аутентификации

i. `RSAAuthentication yes`

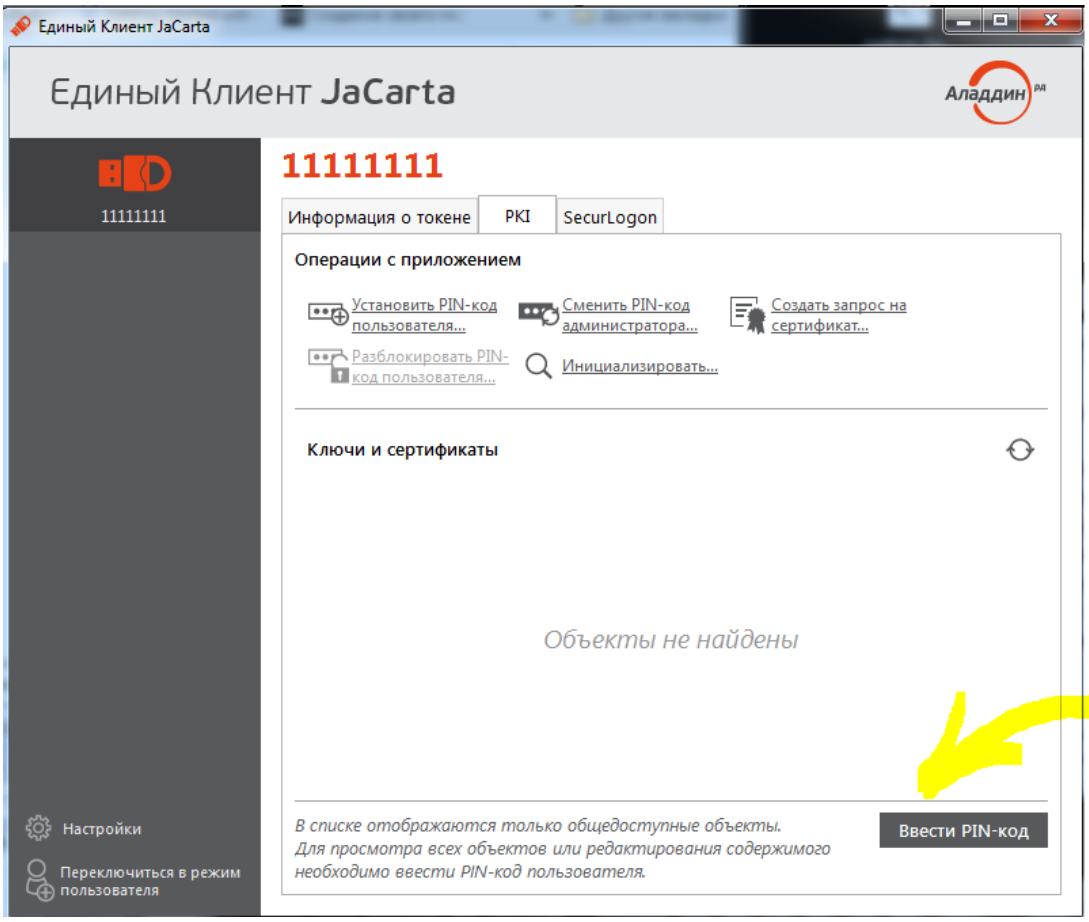
ii. `PubkeyAuthentication yes`

iii. `PasswordAuthentication no` - отказ от аутентификации по паролю (опционально)

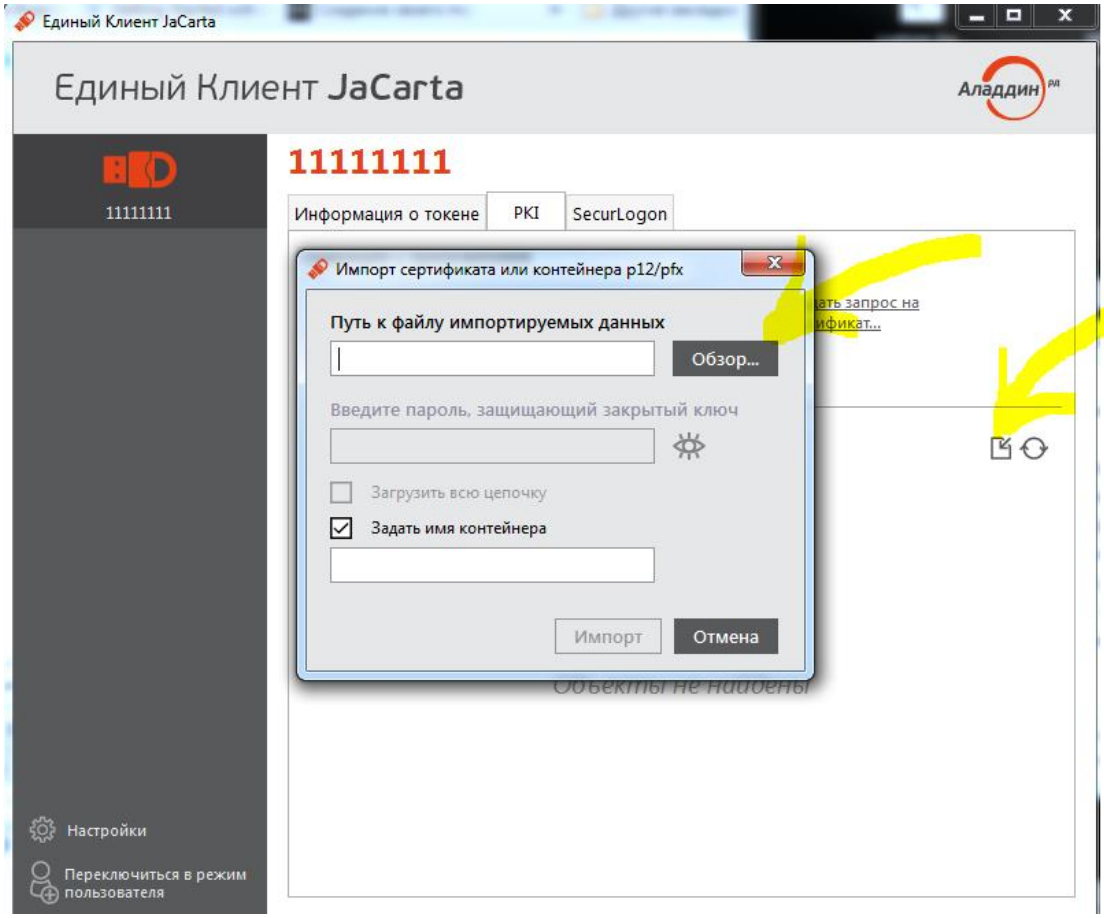
Запись сертификата на смарт-карту

Необходимо перенести сертификат на смарт-карту. Для переноса мы соберем все необходимые объекты в зашифрованный контейнер и записать его на смарт-карту.

- `openssl pkcs12 -export -in user.crt -inkey key -certfile ca.crt -name "user" -out user.pfx`
- Перенос файла user.pfx на Windows систему с установленным Единым клиентом, либо JC Client
- Ввод пин-кода пользователя



- Импортировать сертификат на токен



- Выбрать файл user.pfx и нажать Импорт

Проверка работоспособности сертификата

ssh -I /usr/lib/x86-athena/libASEP11.so 127.0.0.1

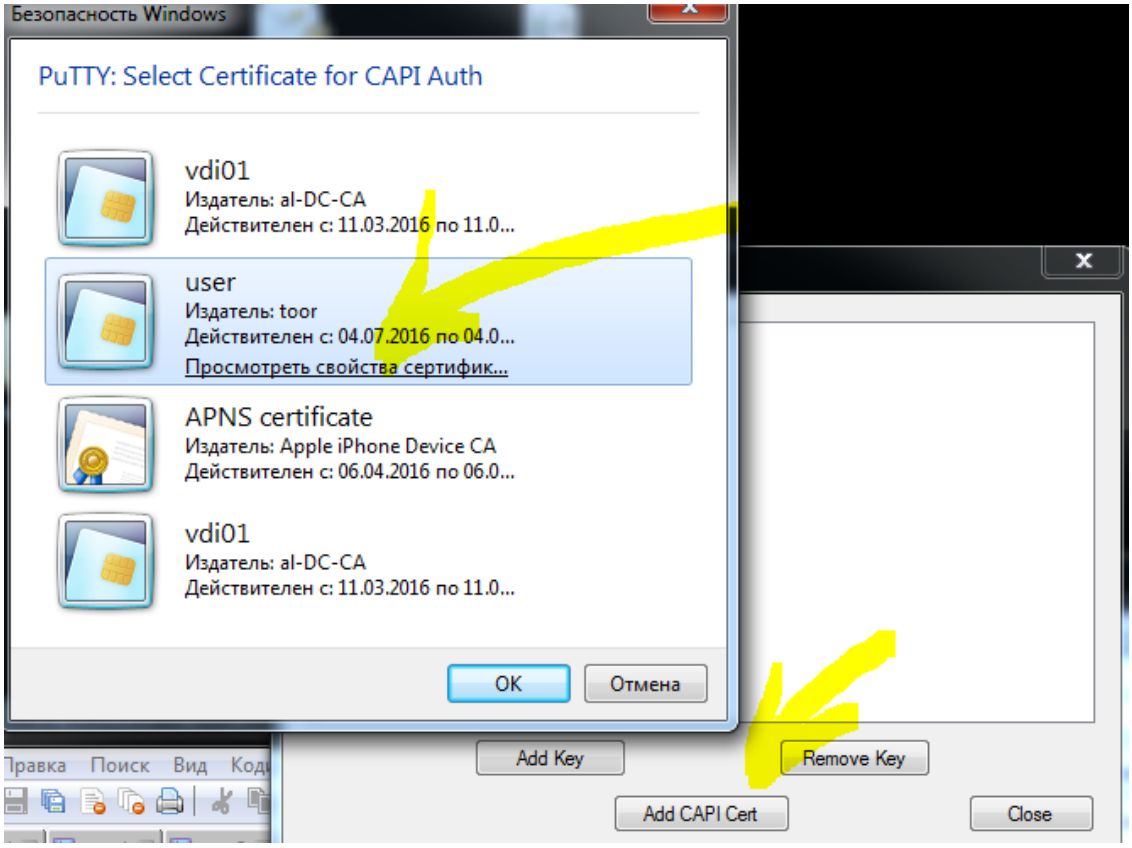
Настройка SSH-клиента Putty на ОС Windows

Запуск утилит из дистрибутива putty-cac\executables

- pageant.exe
- putty.exe

⚠ Для работы требуется версия putty-cac 0.62

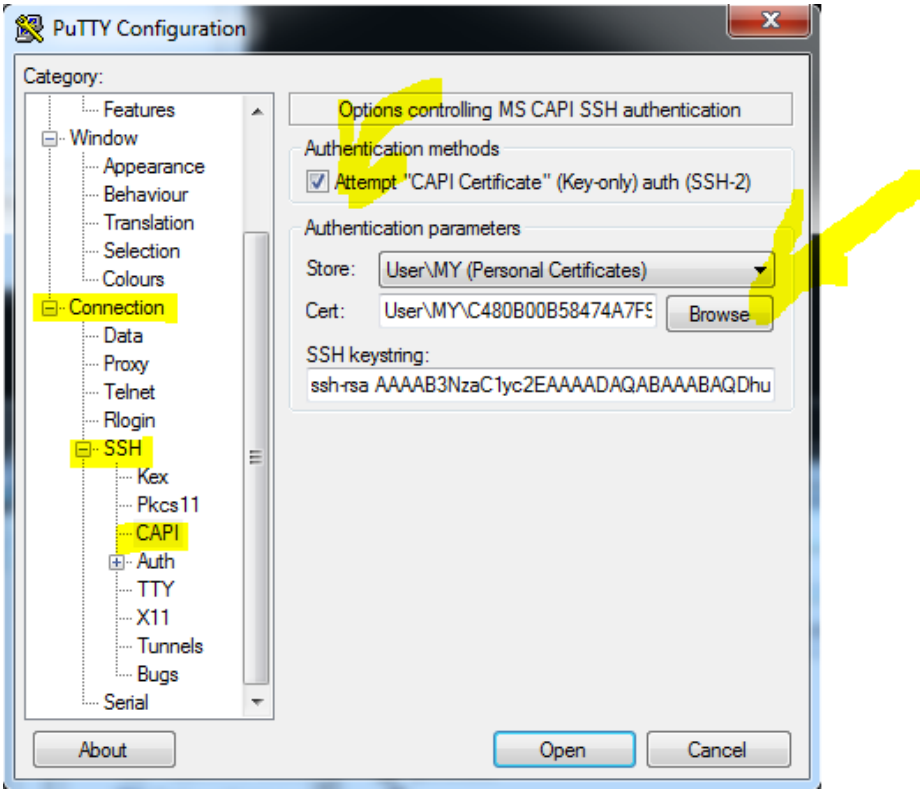
Выбор сертификата в pageant



⚠ В общем случае сертификат появляется в хранилище сертификатов автоматически, но в некоторых случаях может потребоваться его добавление вручную.

Запуск и настройка Putty

Вкладка Connection/SSH/CAPI


PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Pkcs11
CAPI
Auth
TTY
X11
Tunnels
Bugs
Serial
Options controlling MS CAPI SSH authentication
Authentication methods
Attempt "CAPI Certificate" (Key-only) auth (SSH-2)
Authentication parameters
Store:
User\MY (Personal Certificates)
Cert:
User\MY\C480B00B58474A7F
Browse
SSH keystring:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhu
About
Open
Cancel

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания «Аладдин Р. Д.».

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: aladdin@aladdin-rd.ru (общий).

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений[1]

Версия	Изменения
1.0	
0.9	
0.1 dra☐	Создание документа

[1] *Нотация: более крупным и ярким делается только первая строка, относящаяся к текущей (актуальной версии документа). Ранее сделанные изменения (история) оформляется более мелким серым курсивом.*

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Microsoft Silver OEM Hardware Partner, Microsoft Silver Cloud Platform Partner, Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru