JaCarta PRO и платформа Teradici

Аутентификация в сессию VMware Horizon по аппаратному PCoIP

Листов: 18

Автор: Dmitry Shuralev

Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации в сессию **VMware Horizon View** с использованием смарт-карт и USB-токенов **JaCarta PRO** на нулевых тонких клиентах с архитектурой **Teradici** и аппаратной реализацией протокола **PCoIP.**

Оглавление

PCoIP и технология Teradici

PCoIP – это ориентированный на сервер протокол, что означает, что большинство операций по визуализации графики и обработке данных выполняется на мощных серверах, а не локальных компьютерах. Битмапы или кадры передаются на удалённые клиенты с компрессией. Не секрет, что прежде протоколы удалённой работы не были идеальным решением в сравнении с локальным выполнением операций на клиентском ПК. Однако централизованное управление и безопасность представляют собой настолько поразительные преимущества, что легко компенсируют этот недостаток. **PCoIP** – это протокол удалённой работы с графикой, разработанный компанией Teradici и реализованный в спектре аппаратных решений. Компания VMware тесно сотрудничала с Teradici, создавая виртуализированную реализацию этого надёжного инновационного протокола и обеспечивая превосходную работу с удалённым рабочим столом в VMware Horizon View.

Технология PC-over-IP предлагает набор встроенных возможностей для обеспечения безопасности. 100% вычислений переносятся в защищённый центр обработки данных – сами данные никогда не покидают центр, при передаче данных внутри центра используется шифрование.

Протокол PC-over-IP сжимает, шифрует и кодирует данные при работе с центром обработки данных, а также передаёт их в формате только пикселей по стандартной IP-сети к рабочим компьютерам с поддержкой PCoIP. Технология PC-over-IP позволяет централизованно управлять компьютерами на предприятиях и рабочими станциями непосредственно из центра обработки данных, обеспечивая работу с данными высокого разрешения, 3D графикой с высокой скоростью смены кадров и HD медиаданными, поддерживая использование периферийных USB-устройств, локально в LAN или удалённо по беспроводной сети (WAN).

Используя совместно с этим и электронные ключи **JaCarta PRO**, можно дополнительно повысить безопасность предприятия и получить дополнительные плюсы.

В **firmware Teradici** на низком уровне обеспечена поддержка USB-токенов и смарт-карт **JaCarta PRO**, это позволяет работать с USB-токенами и смарт-картами "из коробки" без установки дополнительного ПО или сложных настроек. Поддержаны сценарии:

- аутентификации в терминальные сесии **VMware Horizon View** по сертификатам, хранящимся на **JaCarta PRO;**
- блокировка терминальной сессии при отключении токена или смарт-карты от тонкого клиента;
- проброс токена и смарт-карты в терминальную сессию и работа с ним внутри сессии с любым прикладным ПО, поддерживающим смарт-карты и токены, включая и ГОСТ-алгоритмы при пробросе **JaCarta ГОСТ.**

Описание демо-стенда

Инфраструктура

Тесты проводились в инфраструктуре VDI — VMware Horizon View версии 7.

Инфраструктуры PKI, vSpere и View развёрнуты на базе серверов Microsoft Windows Server 2012 R2 в рамках гипервизора VMware esxi.

Тонкий клиент

Тонкий клиент ТОНК 1100z на чипе Teradici, прошивка версии 5.0.0.

Список поддерживаемых тонких клиентов

Любой нулевой тонкий клиент на чипе **Teradici.**

⚠ Протестированная модель и версия прошивки **Teradici — ТОНК 1100z, firmware 5.0.0.**

Список поддерживаемых USB-токенов и смарт-карт

Для аутентификации в сессию VMware Horizon View

JaCarta PRO – USB-токен

JaCarta PRO – смарт-карта

Проброс ключа в сессию и работа с ним внутри сессии

JaCarta PKI – USB-токен

JaCarta PKI – смарт-карта

JaCarta PKI/ГОСТ – USB-токен

JaCarta PKI/ГОСТ – смарт-карта

JaCarta PKI/Flash – USB-токен

JaCarta PKI/ГОСТ/Flash – USB-токен

Поддерживаемые считыватели смарт-карт

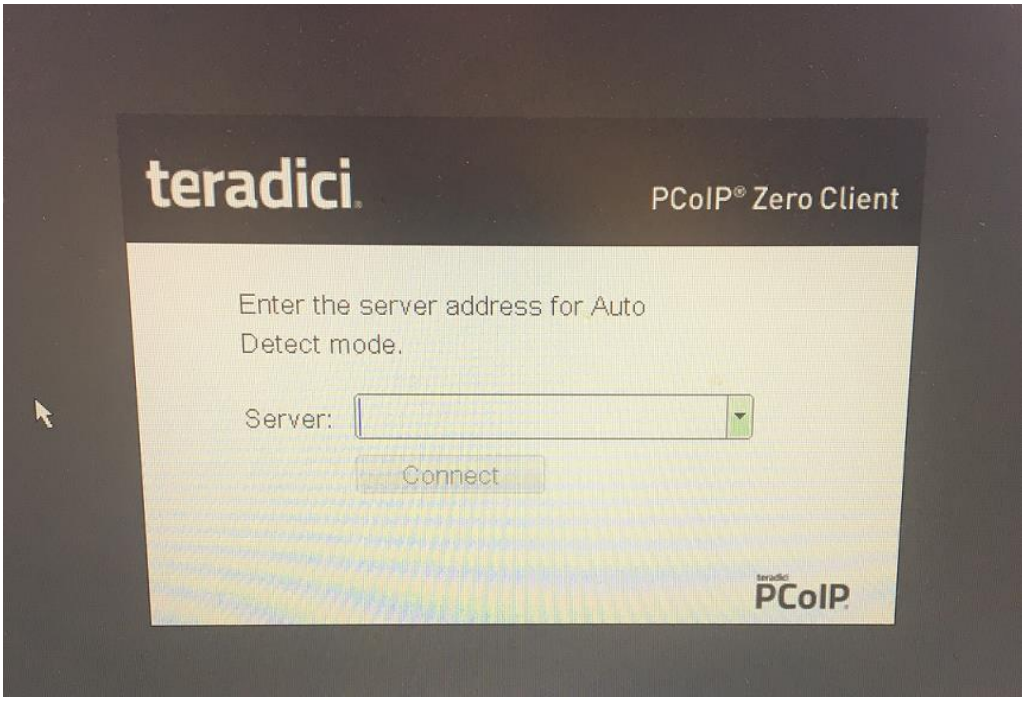
ASEDrive IIIe USB

ASEDrive IIIe USB mini

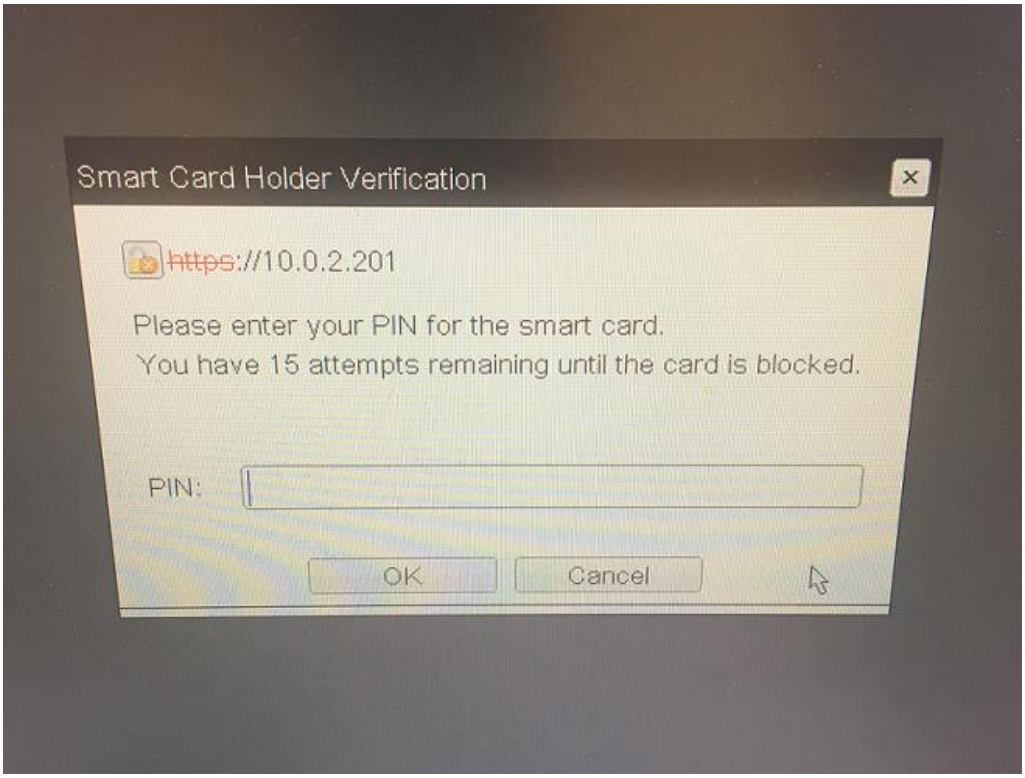
Настройка тонкого клиента

Как было сказано ранее, поддержка **JaCarta PRO** в прошивках **Teradici** осуществлена на низком уровне, и электронные ключи определяются системой сразу, что называется "из коробки".

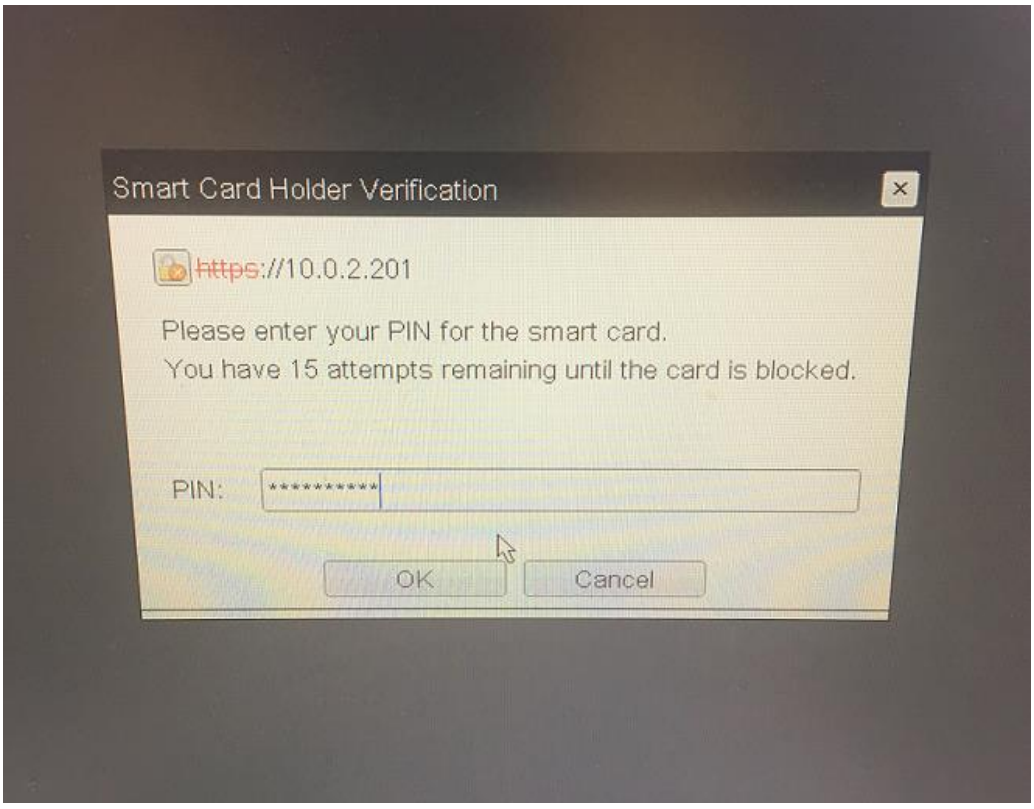
В поле Server введите адрес брокера **VMware Horizon View.**



При подключенном USB-токене или смарт-карте при запросе брокера **Horizon View** система сама определит, что электронный ключ подсоединён и попросит ввести PIN-код.

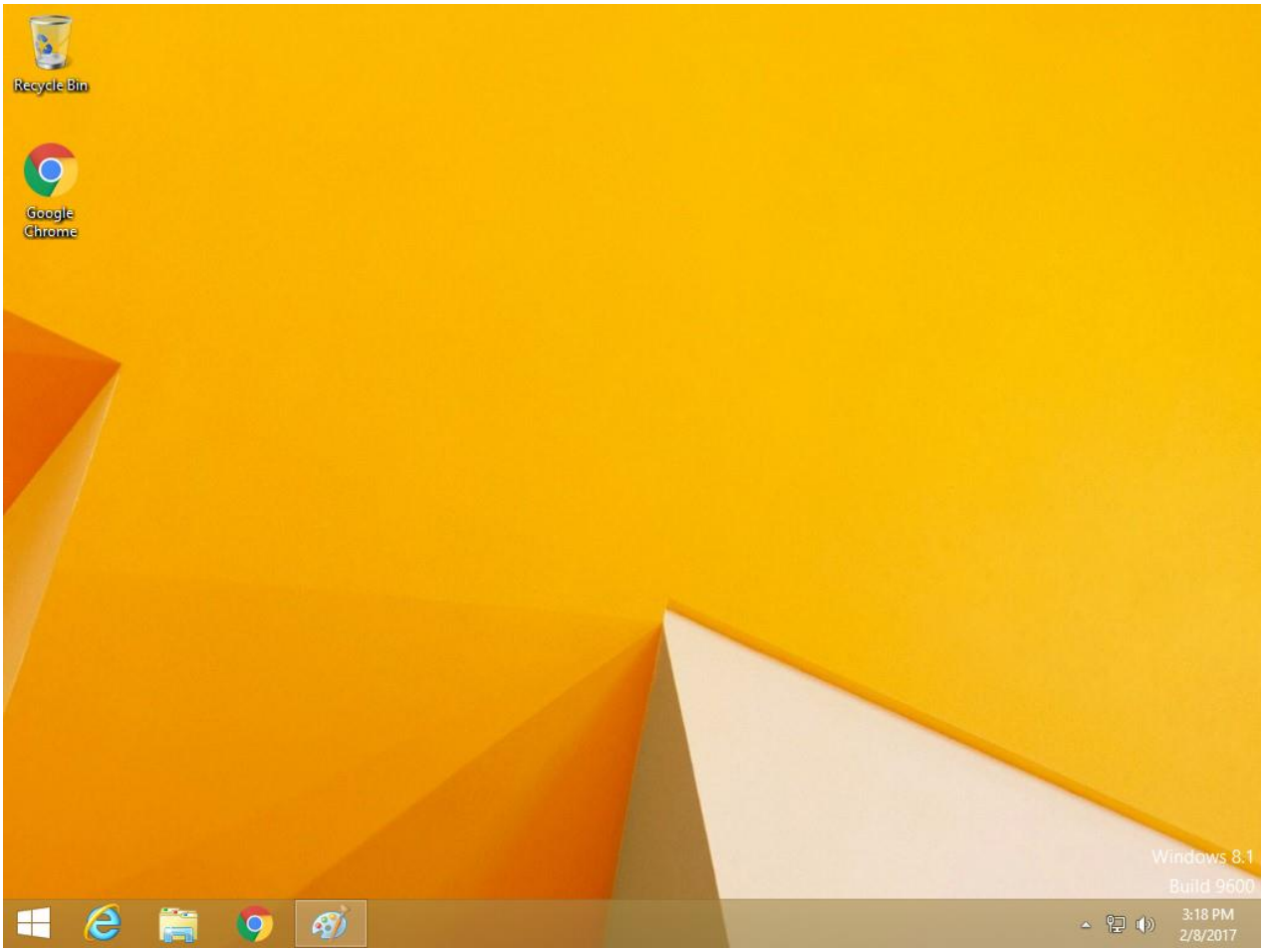


Введите PIN-код.

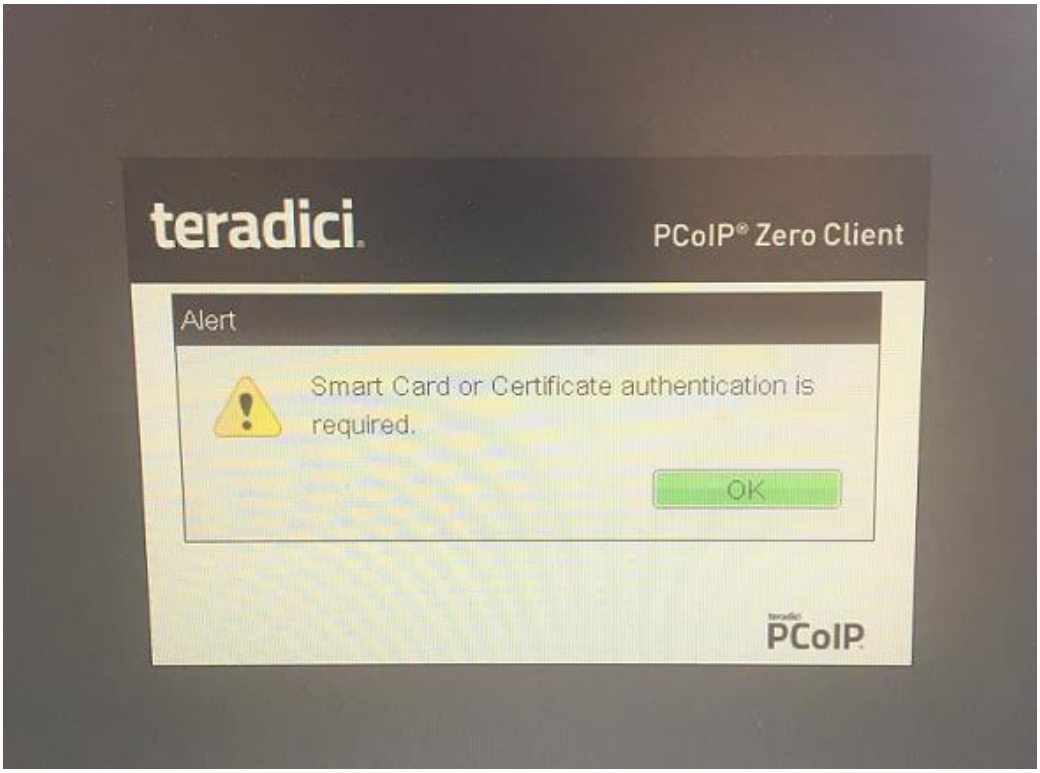


Отобразится доступный пул ресурсов, выберите необходимый десктоп.

Далее произойдёт соединение с нужным рабочим столом.



Если со стороны сервера **VMware Horizon View** стоит настройка — вход только по смарт-карте и традиционный вход по паре логин/пароль отключен, а сама смарт-карта не подключена, — то отобразится следующее окно.



В этом случае необходимо подключить смарт-карту или электронный ключ и ввести его PIN-код.

Сертификат корневого центра сертификации

Проверка сервера

В системе **Options -> User Settings -> Certificate** существует несколько опций проверки сервера, согласно которым выполняются или не выполняются некоторые функции.

1. **Never Connect to untrusted servers (Никогда не подключаться к недоверенным серверам).**
2. **Warn Before connecting to untrusted servers (Сообщать перед подключением к недоверенному серверу).**
3. **Do not verify server identity certificates (Не проверять сертификат сервера).**

Чтобы работать по первой или второй схеме, необходимо, чтобы система знала о корневом центре сертификации, выдавшем сертификат на токен или смарт-карту.

Добавление корневого сертификата в хранилище

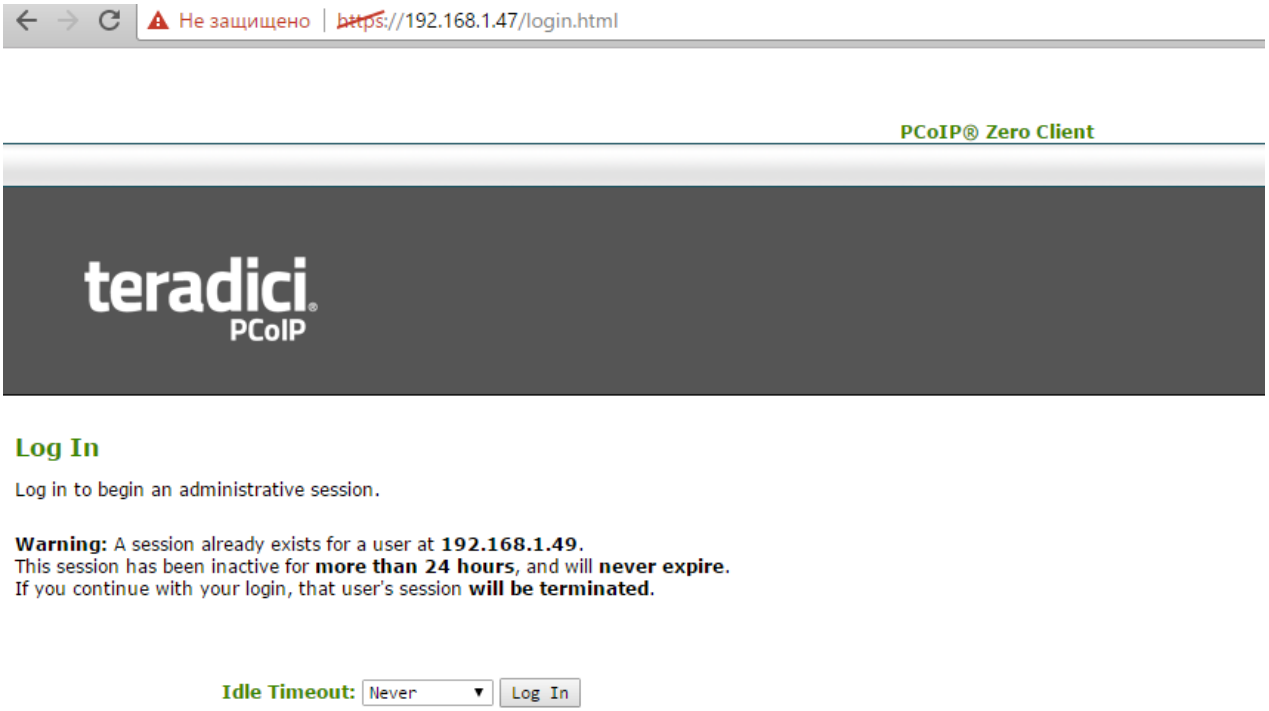
Если сертификат на токене или смарт-карте выдан недоверенным или неизвестным центром сертификации, необходимо поместить сертификат корневого и промежуточных (при их наличии) Удостоверяющих центров в собственное хранилище **Teradici** для правильного построения цепочки сертификатов.

Чтобы попасть в хранилище, необходимо подключиться к тонкому клиенту через Web-интерфейс со стороннего компьютера, по адресу: https://IP-адрес,

где IP-адрес - это полученный по DHCP или настроенный вручную адрес тонкого клиента Teradici.

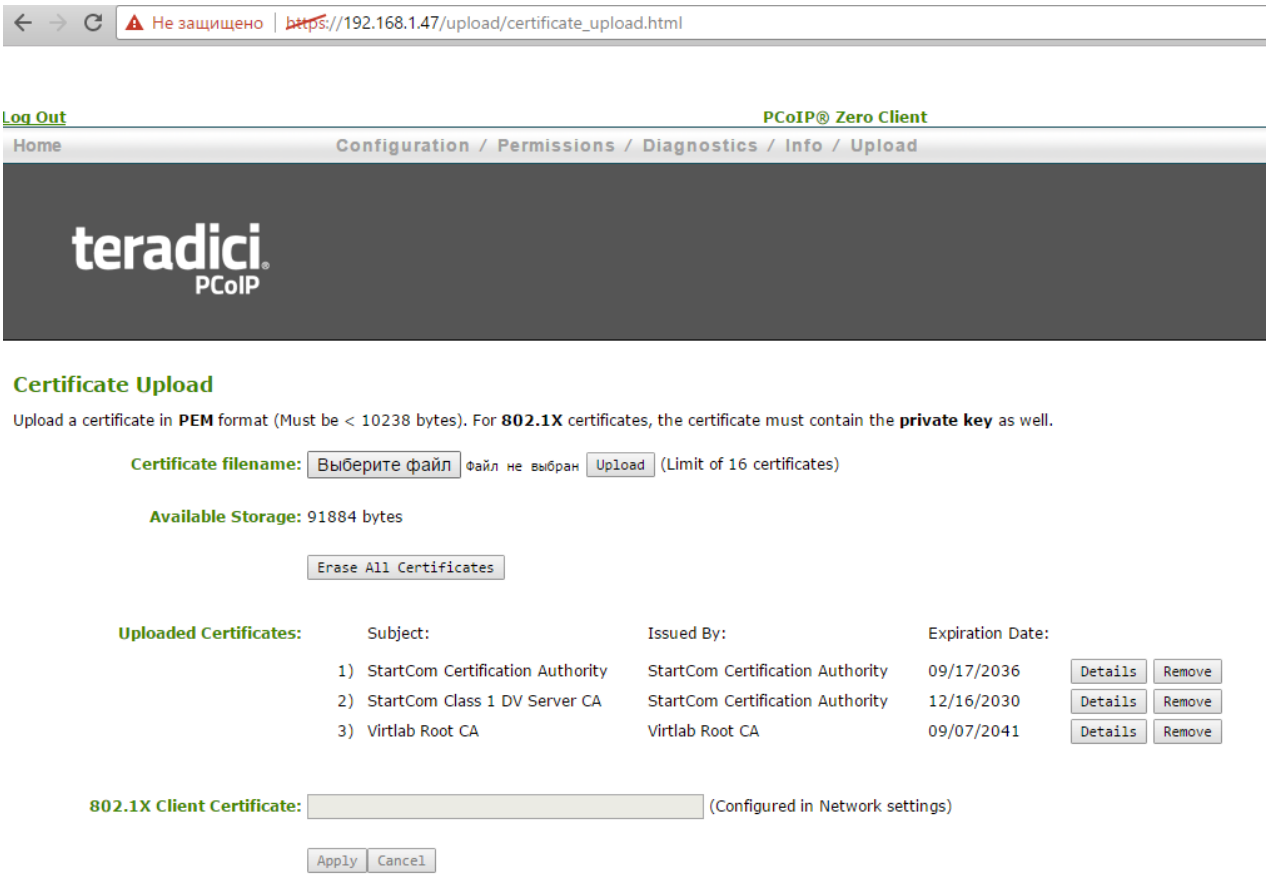
Этот адрес можно посмотреть на самом тонком клиенте, через меню **Options -> Configuration -> Network.**

В отобразившемся окне нажмите **Log In.**



Отобразится главное окно конфигурации с различными настройками. Выберите **Upload -> Certificate.**

В следующем окне выберите файл сертификата **Certificate filename Выберите файл,** выберите нужный сертификат и нажмите **Upload.**

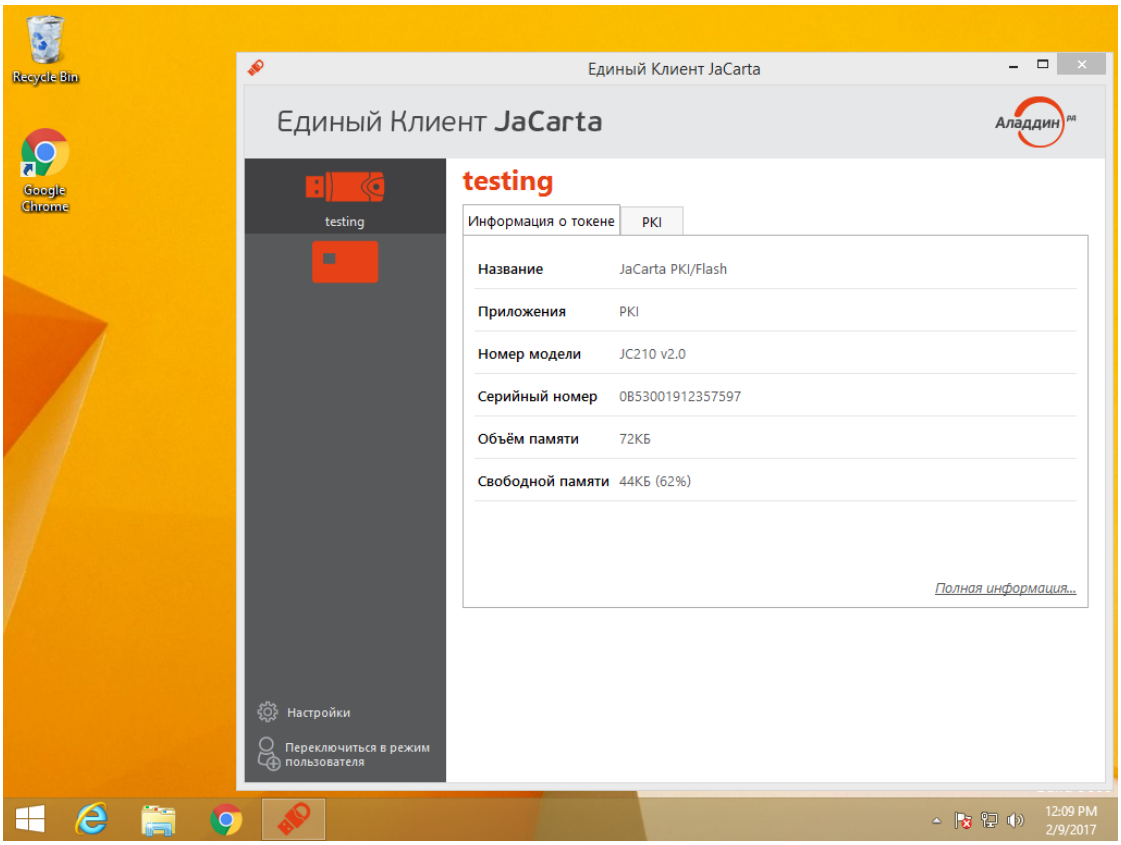


После того, как сертификаты будут добавлены, можно подключаться к серверу по схеме 1 и по схеме 2 без предупреждений безопасности.

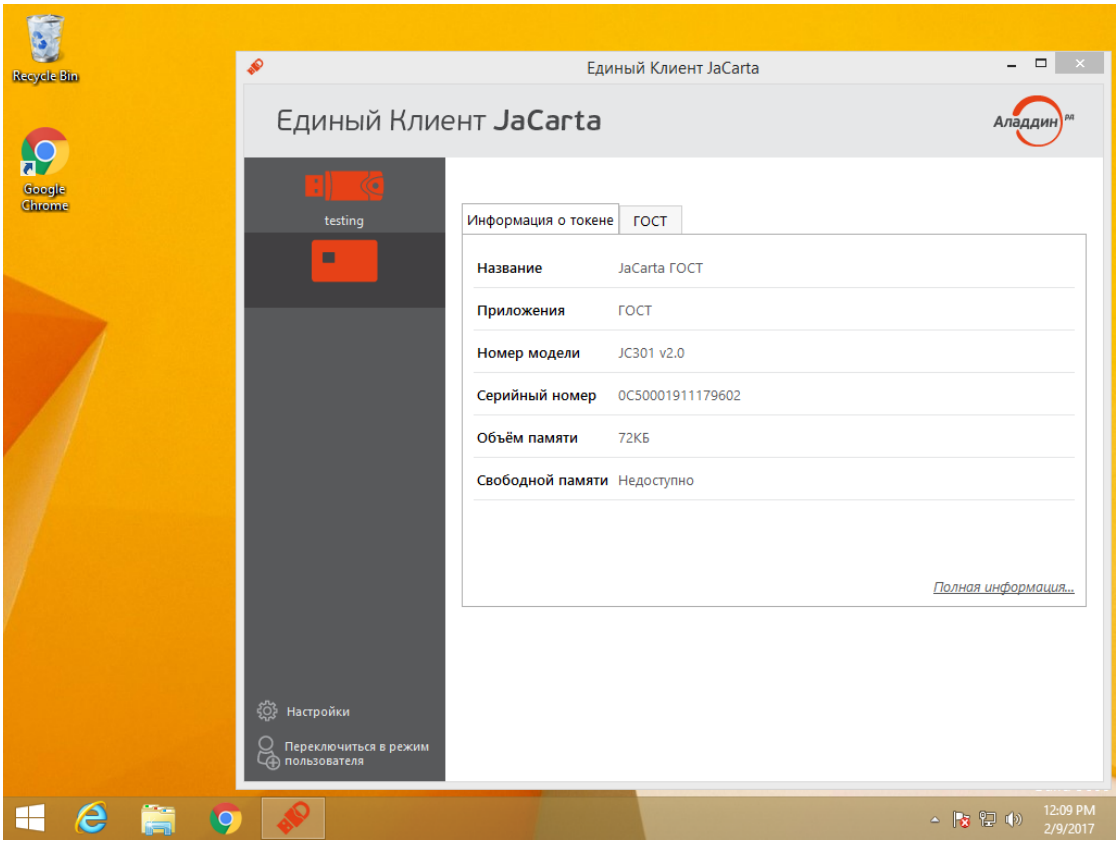
Зелёная надпись https:// с зелёной галкой подтверждает, что сертификат сервера проверен.

Работа с JaCarta внутри терминальной сессии, поддержка JaCarta ГОСТ

USB-токены и смарт-карты **JaCarta** пробрасываются в терминальную сессию, и у пользователя есть возможность работы со смарт-картой или токеном в любых приложениях, поддерживающих такую функциональность. Это могут быть стандартные для Microsoft Windows приложения, например, — RDP, EFS, VPN, пакеты MS Office, защита электронный почты Outlook, доступ к корпоративным порталам Outlook Web Access и SharePoint. Или стороннее ПО, например, — КриптоПро CSP, VipNet CSP; Web-сайты, банк-клиенты и многое другое.



Также пробрасываются и смарт-карты и токены линейки ГОСТ.



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 Web-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

Версия	Изменения
1.0	Исходная версия документа

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
Apple Developer

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