SSL сертификаты для ECS

Современные браузеры открывают соединения к сторонним серверам только по защищенным протоколам: HTTPS или в нашем случае WSS.

Для открытия WSS соединения нужно, чтобы на сервере (взаимодействия) был валидный SSL сертификат, которому доверяет браузер пользователя.

Сертификаты сервера хранятся в хранилище в формате JKS.

Терминология

JKS (Java Key Store) - хранилище сертификатов в Java формате.

Ключевая пара - приватный ключ и связанный с ним сертификат.

Особенности

Современные браузеры требуют в сертификате наличия расширения SAN (Subject Alternative Name)

Создание JKS-хранилища для существующей ключевой пары

Предположим следующее:

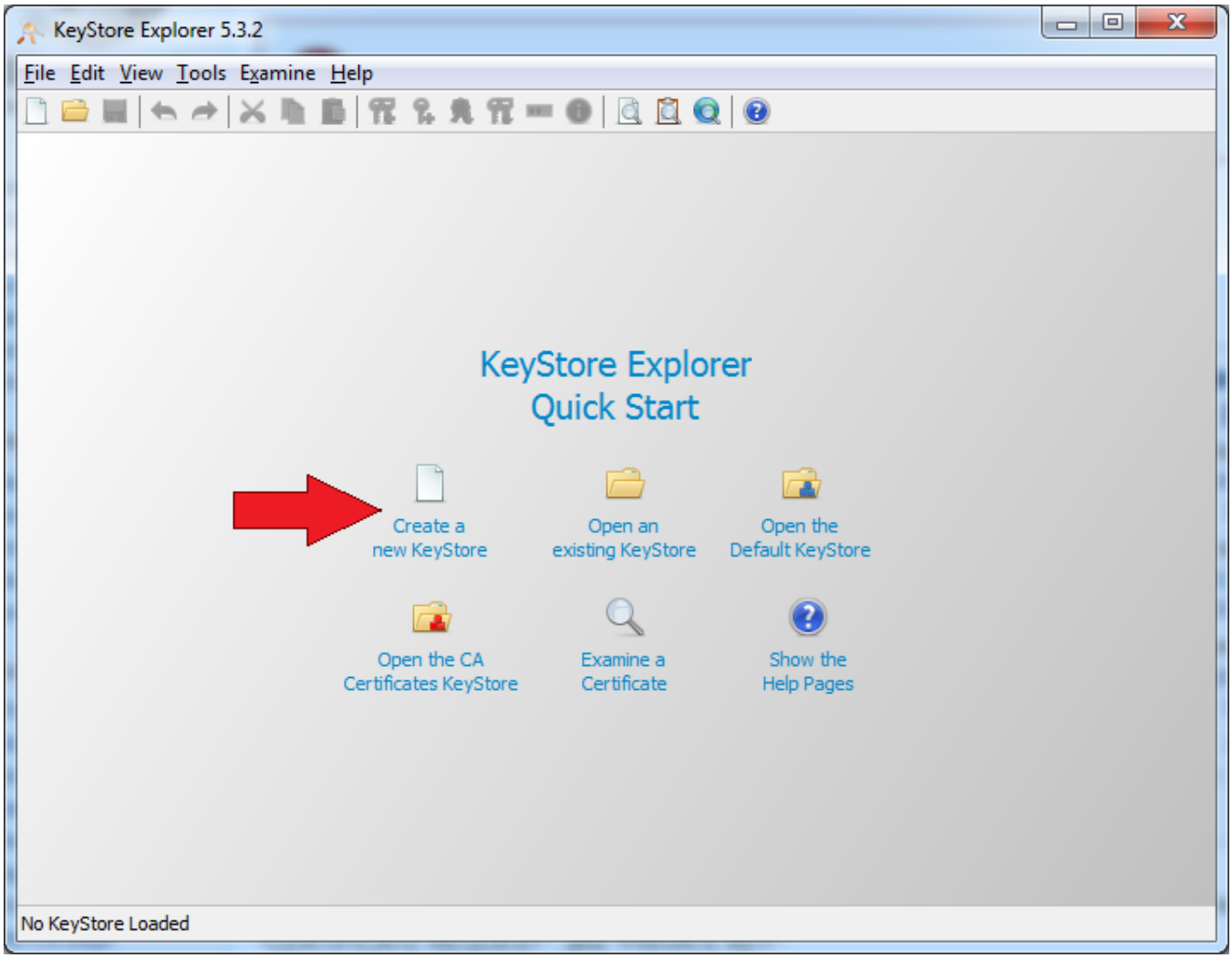
- mydomain - название домена, на котором работает сервер взаимодействия
- mydomain.key - файл, содержащий приватный ключ, в PEM-формате
- mydomain.crt - файл, содержащий сертификат, в PEM-формате, выписанный для домена mydomain

Шаг 1. Установка утилит

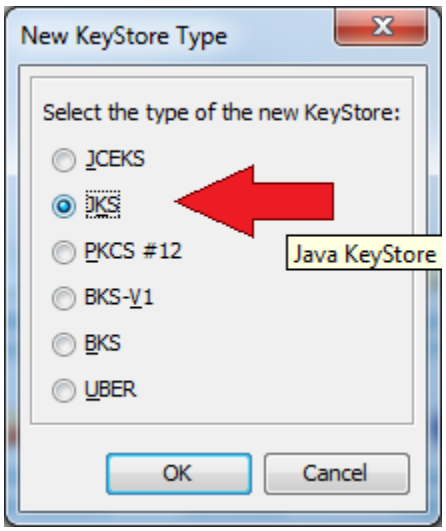
Скачайте утилиту Keystore Explorer, установите и запустите ее.

Шаг 2. Создание нового хранилища

Нажмите на иконку создать новое хранилище

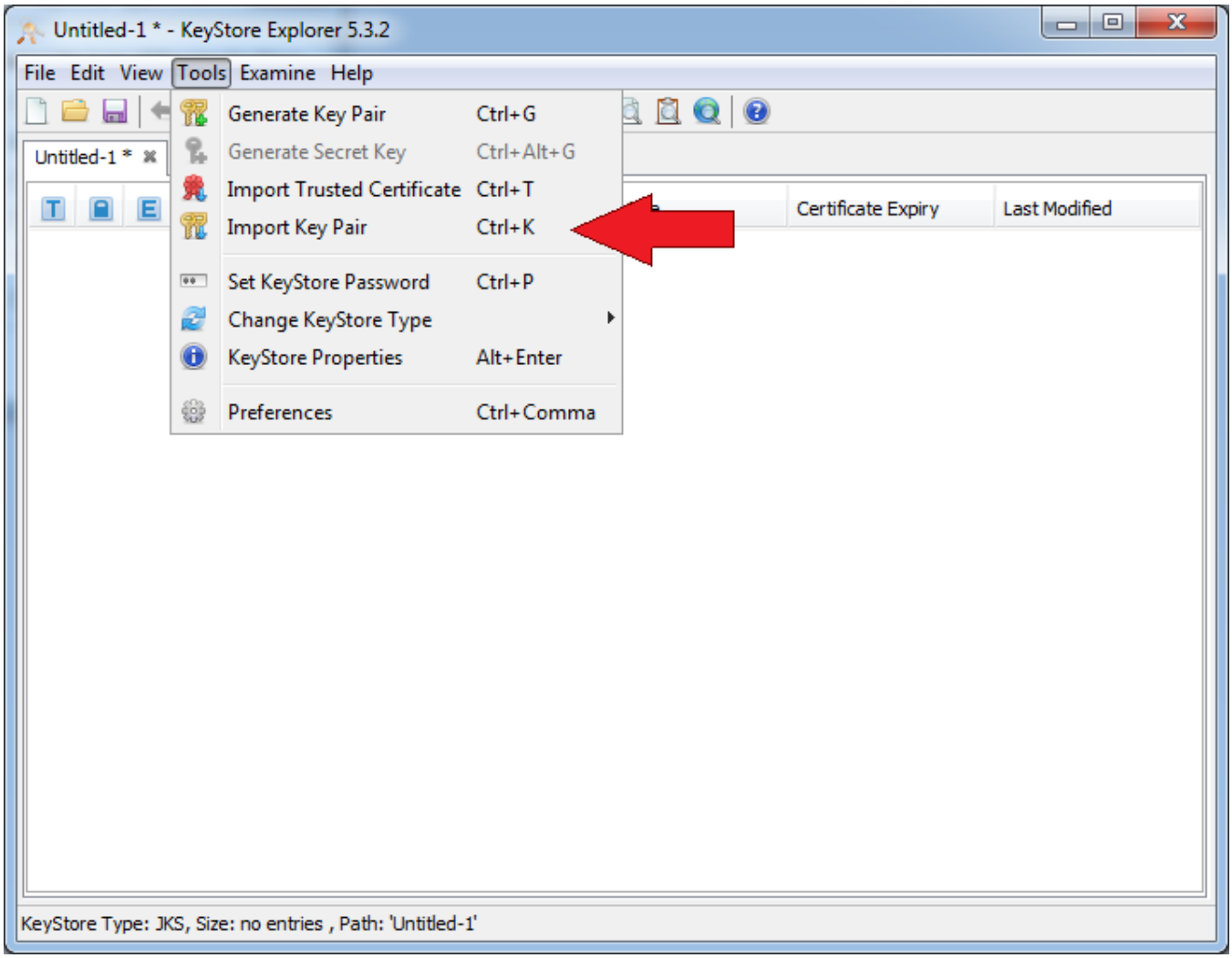


В диалоговом окне выберите тип JKS и нажмите OK

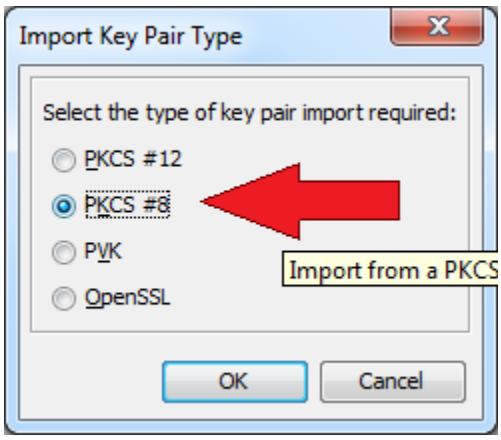


Шаг 3. Импорт ключевой пары

В верхнем меню выберите пункт Import Key Pair



В диалоговом окне выберите тип PKCS #8 и нажмите OK

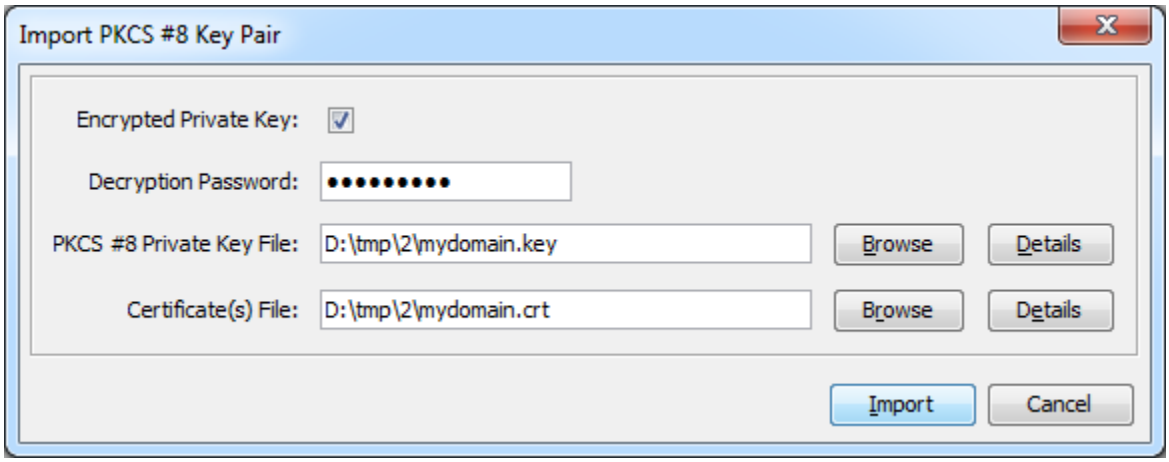


В появившемся диалоговом окне укажите файл, содержащий приватный ключ и файл сертификата.

В поле Decription Password введите пароль приватного ключа.

Кнопка Details покажет информацию по каждому из файлов или информацию о возникших ошибках при открытии файлов

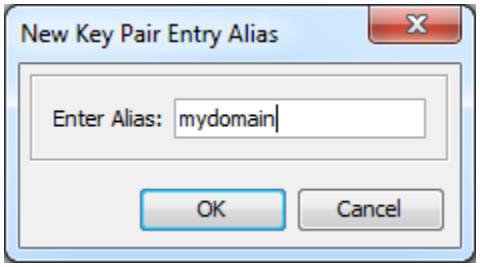
Если ошибок нет, то нажмите кнопку Import



В появившемся диалоговом окне введите имя (alias) ключевой пары и нажмите OK.

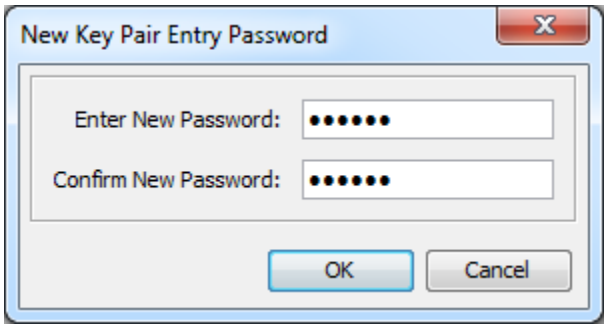
Важно! Имя ключевой пары должно совпадать с доменом, на котором работает сервер взаимодействия.

В нашем случае это mydomain

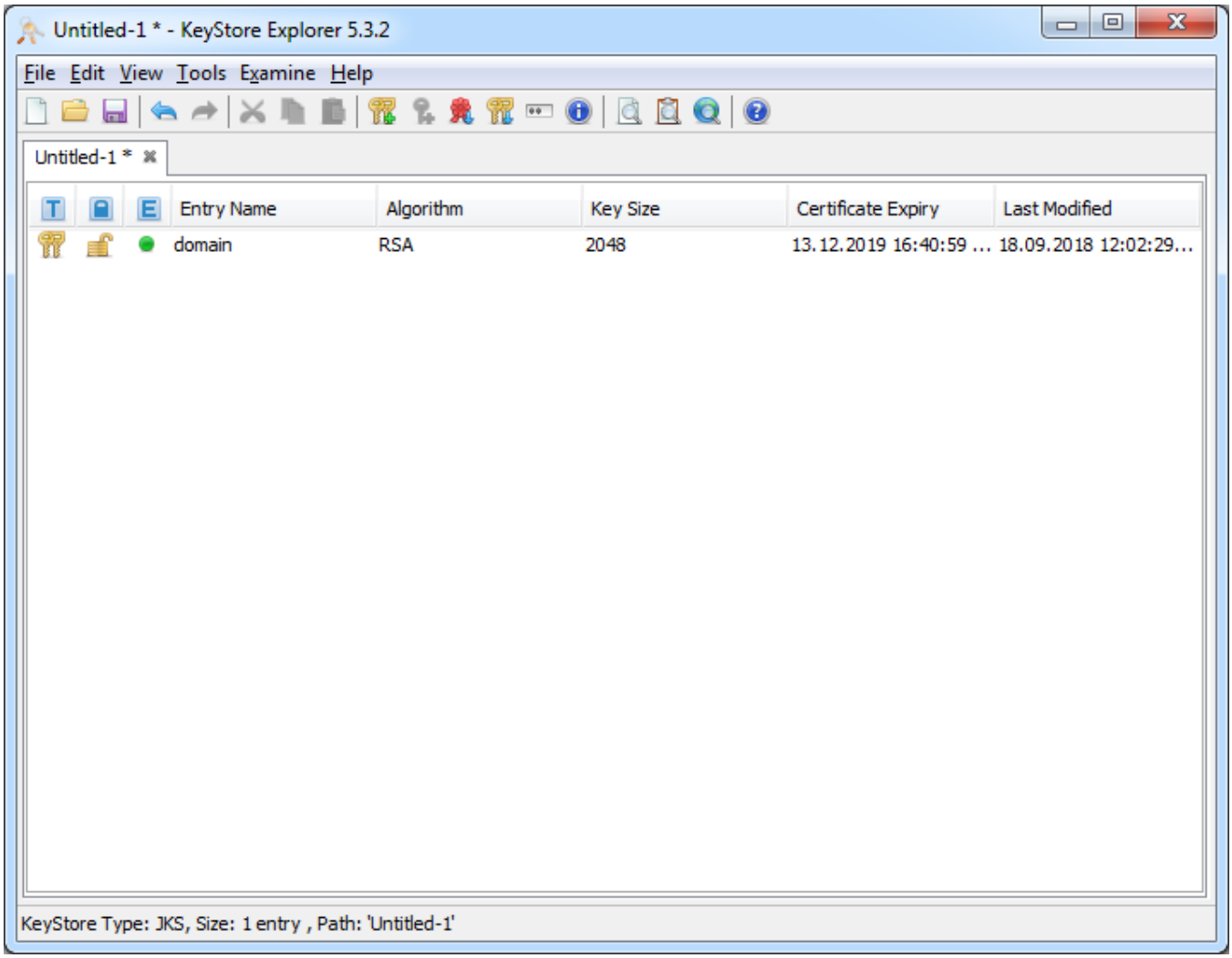


В появившемся диалогом окне введите пароль для ключевой пары и нажмите OK

Важно! Пароль ключевой пары должен совпадать с паролем, которым зашифрован приватный ключ.



В итоге в хранилище должна появится запись с ключевой парой для домена mydomain



Шаг 4. Сохраните хранилище в файл