Инструкция по созданию защищённого канала связи с помощью SSL

Оглавление

Вступление

Протокол SSL обеспечивает защищенный обмен данных за счет двух следующих элементов:

- Аутентификация
- Шифрование

SSL использует асимметричную криптографию для аутентификации ключей обмена, симметричный шифр для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

Протокол SSL предоставляет "безопасный канал", который имеет три основных свойства:

1. Канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.
2. Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, а клиентская делает это опционно.
3. Канал надежен. Транспортировка сообщений включает в себя проверку целостности.

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложений (HTTP, FTP, TCP и т.д.) могут работать поверх протокола SSL совершенно прозрачно, т.е. SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того, как приложение примет или передаст первый байт сообщения.

Рассмотрим поэтапное создание защищенного соединения по средствам SSL сертификации на примере «Сервер данных» – «Касса».

Создание такого соединения предполагает три основные этапа:

1. Создание трех типов сертификатов (корневой, серверный и клиентский).
2. Импортирование сертификатов в соответствующее хранилища
3. Настройка приложений.

Ниже рассмотрим каждый из этих этапов более подробно.

Создание сертификатов

Для создания SSL сертификатов в комплексе «OpenStore» используется приложение «Менеджер сертификатов безопасности», по умолчанию данное приложение находится по следующему пути: «Пуск» - «OpenStore» - «OpenStore» - «Инструменты».

Основное окно приложения (Рисунок 1) состоит из двух областей, в верхней части окна создаются корневые сертификаты, в нижней серверные и клиентские. Кроме этого в правой части окна находятся функциональные кнопки, которые позволяют создавать, удалять, а также экспортировать выбранные сертификаты.

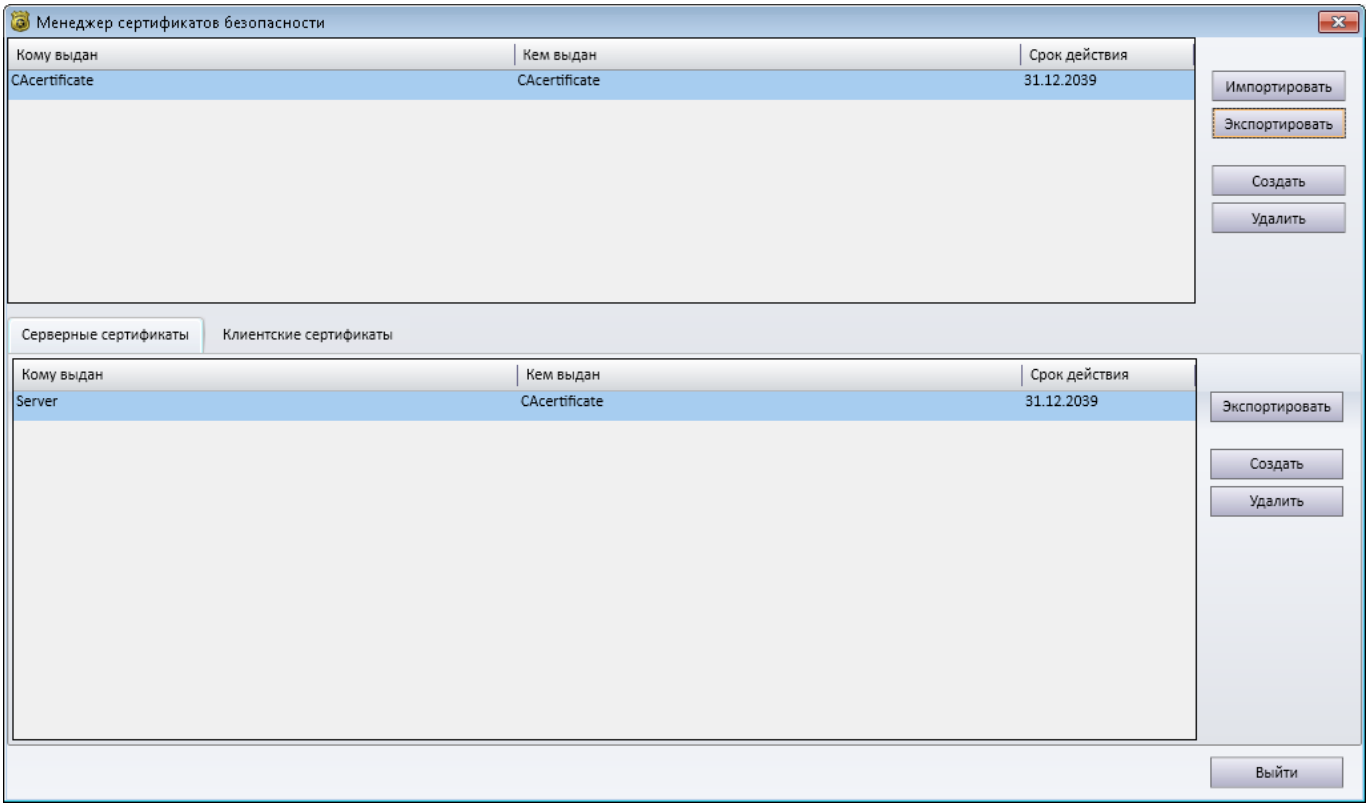

Рисунок 1 «Менеджер сертификатов безопасности»

После того как приложение было запущено в первую очередь создается корневой сертификат, для этого в верхней области окна нажмите кнопку «Создать», появиться окно создания корневого сертификата, в строке «*Издатель сертификата*» следует ввести логические имя для создаваемого объекта. Обратите внимание, что в названии не допускается использование кириллических символов и

символа пробел. Кроме названия сертификата необходимо указать срок его действия, по умолчанию указывается 2040 год, по истечению указанного срока корневой сертификат и сертификаты, относящиеся к нему, будут не действительны.

Нажав кнопку «Принять», вы перейдете в следующее окно, где необходимо указать пароль для данного сертификата, пароль может состоят из цифробуквенных символов латинского алфавита, использование кириллических символов недопустимо. Пароль следует ввести три раза, первые раз создав его, второй и третий раз являются подтверждением. Указанный пароль будет необходим при экспортировании/импортировании сертификата, а также на этапе создании серверных и клиентских сертификатов. Кроме этого существует возможность создавать сертификаты без ввода пароля, кнопка «Отсутствует» на этапе создания пароля закрытого ключа, но такой подход приведет к понижению уровня безопасности защищенной сети.

Завершив с созданием корневого сертификата следует приступить к созданию серверного и клиентского сертификатов. Так как принцип создания серверного и клиентского сертификатов не отличается подробно рассмотрим создание только серверного сертификата.

Для этого в нижней части окна выберете вкладку «Серверные сертификаты» и нажмите кнопку «Создать» после чего появится окно, в котором, по аналогии с созданием корневого сертификата необходимо указать логическое имя серверного сертификата (латинские символы без пробелов), срок его действия и пароль. Обратите внимание, что при создании пароля в первом и во втором окне указывается пароль серверного сертификата, а в третьем окне следует указать пароль корневого сертификата.

После того как были созданы все необходимые сертификаты, а именно корневой, серверный и клиентский их необходимо экспортировать в соответствующие хранилища.

Экспорт сертификатов для серверного и клиентского приложения отличный друг от друга, поэтому рассмотрим каждый из них отдельно.

Экспорт сертификатов для серверного приложения.

Экспортировать необходимо все три сертификата, но с тем отличием, что корневой и клиентские сертификаты экспортируются без закрытого ключа, в то время как серверный сертификат должен иметь закрытый ключ. Экспортировать сертификаты для серверного приложения (Сервер данных), необходимо каждый отдельно, для этого в приложении «Менеджер сертификатов безопасности» выберите нужный и нажмите кнопку «Экспортировать», далее окна экспорта отличаются друг от друга, поэтому рассмотрим каждое из них отдельно.

- ***Корневой сертификат.*** В окне экспорта выберите путь куда будет сохранен файл, а также установите галочку напротив поля «Экспортировать файл сертификата. *.cer»
- ***Серверный сертификат.*** В первом окне экспорта необходимо ввести пароль серверного сертификата, далее появиться окно мастера экспорта сертификатов нажмите кнопку «Далее», в

следующем окне следует выбрать пункт «Да, экспортировать закрытый ключ», далее оставляете пункт по умолчанию, в следующем окне введите пароль сертификата и в последнем окне выберите путь и имя сохраняемого файла

- ***Клиентский сертификат***. При экспорте клиентского сертификата следует повторить все те же действия, которые были произведены с экспортом серверного с одним лишь отличием, экспортировать необходимо без сохранения закрытого ключа.

Экспорт сертификатов для клиентского приложения

Для упрощения экспорта/импорта сертификатов для клиентского приложения предусмотрена возможность экспортирования нужных сертификатов пакетным файлом с расширением *.xml данный файл будет содержать всю необходимую информацию.

Для такого экспорта в приложении «Менеджер сертификатов безопасности» перейдите во вкладку «Клиентские сертификаты» и нажмите кнопку «Создать пакет», далее в появившемся окне вам необходимо указать путь и имя создаваемого пакета, также следует ввести пароль клиентского сертификата, если вы создавали сертификат без пароля оставьте соответствующее поле пустым. Кроме этого должен в пакет должен быть экспортирован серверный сертификат, галочка в одноименном поле.

Настройки сервера данных

Прежде чем приступить к настройке сервера данных, необходимо импортировать ранее созданные сертификаты в приложение «Менеджер хранилища сертификатов», данной приложение должно быть установлено на ПК вместе с «Сервером данных».

Для импортирования сертификатов запустите приложение «Менеджер хранилища сертификатов». В левой части окна (Рисунок 2) выводится перечень доступных каталогов, в которые необходимо добавить сертификаты и закрытый ключ.

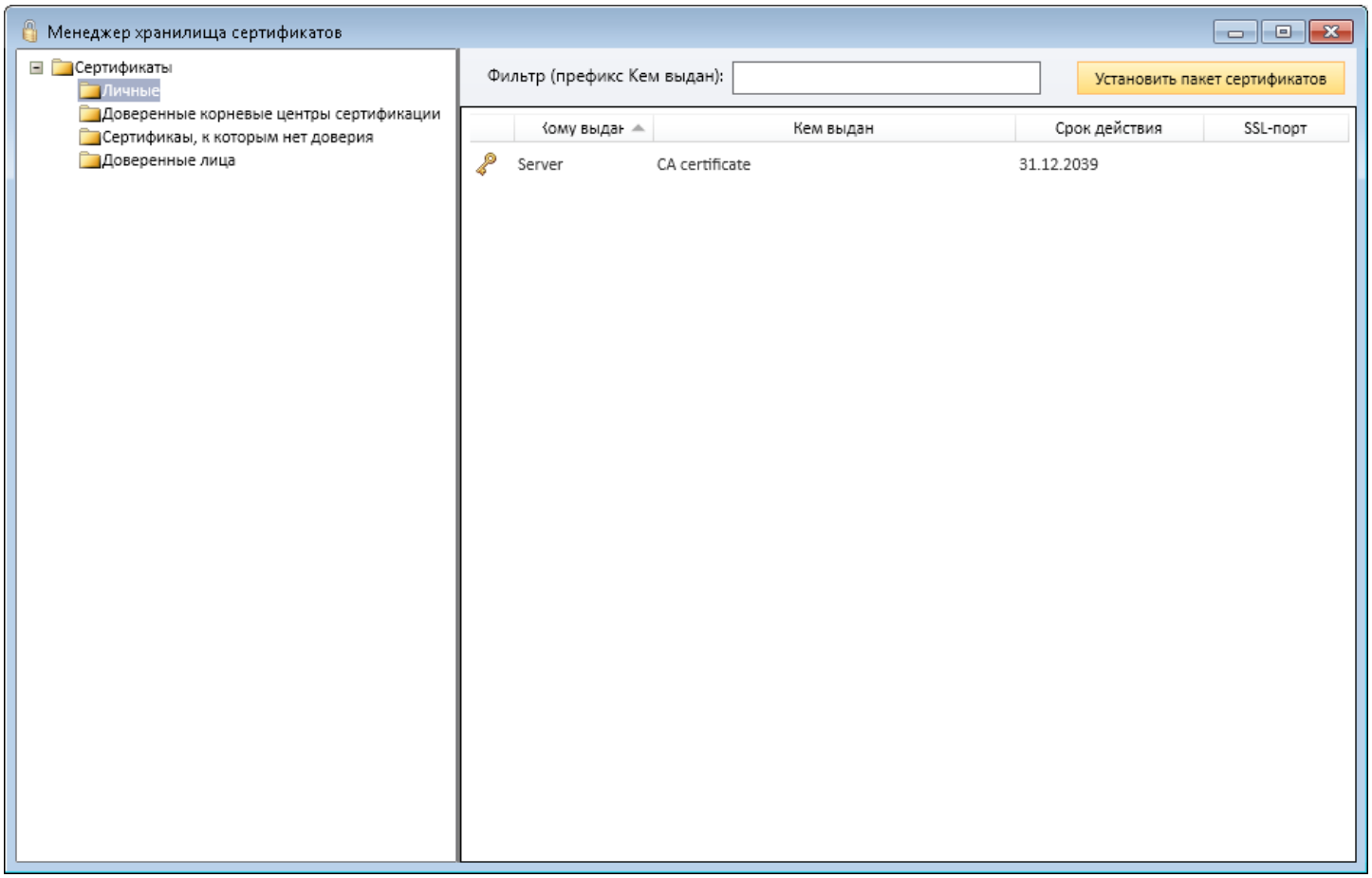

Рисунок 2 «Менеджер хранилища сертификатов»

Рассмотрим более подробно каждый из каталогов.

- «Личные» - в данном каталоге хранятся закрытые ключи серверных сертификатов, файл с расширением *.pfx. Для добавления такого ключа, в правой области выбранного каталога нажмите правую кнопку мышки и выберите пункт «Добавить сертификат», после чего следует выбрать файл с закрытым ключом серверного сертификата, но стоит обратить внимание, что по умолчанию в правом нижнем углу стоит фильтр на файлы с расширениями *.cer, *.crt, поэтому укажите пункт Personal Information Exchange (*.pfx). После добавления данный сертификат будет отображаться в правой области окна.
- «Доверенные корневые центра сертификации» - раздел содержит в себе перечень корневых сертификатов, тут хранятся не только сертификаты, которые будут относится к программному комплексу OpenStore, но и другие сертификаты операционный системы Windows. Добавление

корневого сертификата в данный каталог ничем не отличается от способа, описанного выше, с тем лишь отличием, что фильтр по умолчанию указан правильно.

- «Сертификаты, к которым нет доверия» - раздел должен содержать в себе перечень сертификатов, которые по той или иной причине были дискредитированы.
- «Доверенные лица» - данный раздел содержит в себе перечень всех клиентских сертификатов, файлы с расширением *.cer,

Следует обратить внимание, что при добавлении нового сертификата необходимо вводить ранее созданный пароль того сертификата, который вы добавляете.

После того как все три сертификаты были добавлен следует добавить данные о серверном сертификате в приложении «Сервер данных». Для этого в настройках сервера во вкладке «Общие» в пункте SSL сертификат необходимо указать имя серверного сертификата в строке «Кому выдан», в нашем случае, как видно на Рисунок 1 это имя «Server».

Так же во вкладке «Порты соединений» установите галочку «Использовать SSL» относительного используемого соединения с клиентскими приложениями. Это может быть, как TCP, так и HTTP соединения.

Более подробную информацию о настройках данного приложения вы можете найти в документе «OpenStore.Сервер данных (руководство администратора)».

Настройки клиентского приложения.

В качестве клиентского приложения у нас выступает касса.

Для её настройки, как и с сервером данных необходимо сначала импортировать пакет сертификатов. Для этого запустите приложение «Менеджер хранилища сертификатов» и нажмите кнопку «Установить пакет сертификатов», после чего выберите ранее экспортируемый пакет, который содержит в себе всю необходимую информацию о сертификатах и закрытых ключах. Также на заключительном этапе установки вам необходимо будет ввести пароль клиентского сертификата.

После того как пакет был добавлен каждый из разделов будет заполнен соответствующем это касается всех разделов, кроме раздела «Сертификаты, к которым нет доверия» добавлять дискредитированные сертификаты необходимо отдельно.

Далее можно приступить к настройкам приложения «Касса», а именно в приложении «Касса» перейдите к настройкам локального профиля и во вкладке «Синхронизация» установите галочку «Использовать SSL», после чего будут доступна два поля «SSL-сертификат» и «Удостоверение сервера» заполнить данные поля можно как вручную, так и с помощью SSL пакета, после способ является более предпочтителен. Для импортирования настроек с помощью SSL пакета, нажмите одноименную кнопку и выберите ранее созданный пакет сертификатов, далее следует ввести пароль

клиентского сертификата и подтвердить импорт настроек. В результате поля, относящиеся к SSL сертификации, будут заполнены автоматически. Пример заполнения вы можете увидеть на Рисунок 3.

Подробную информацию о настройках локального профиля кассы вы можете найти в документации «OpenStore.Касса (руководство администратора)».

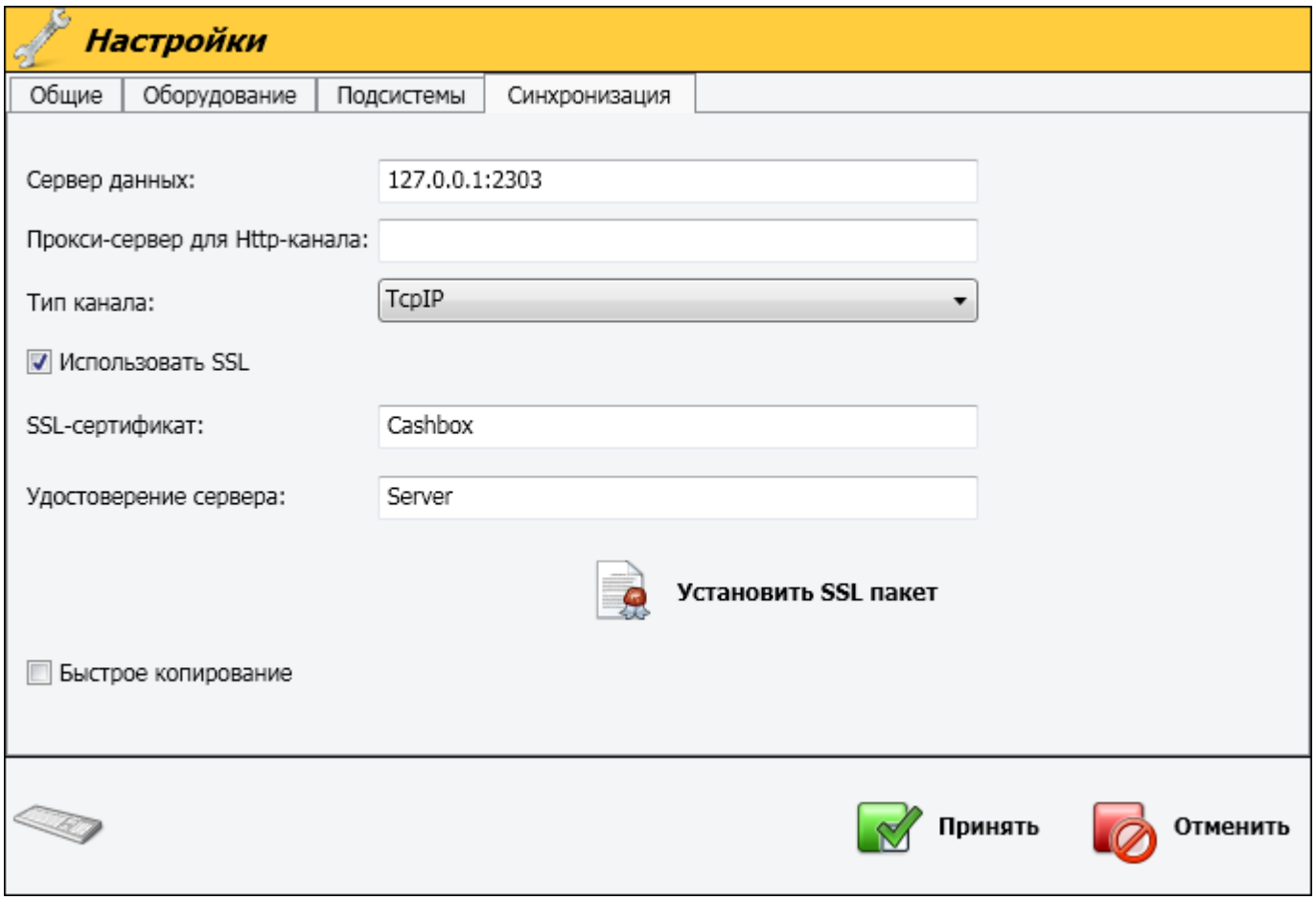

Рисунок 3 Настройки Касса, вкладка «Синхронизация»