**Инструкция по работе с утилитой Stunnel   
из пакета CryptoSCP в Windows системах.**

**1. Описание утилиты**

Утилита stunnel предназначена для шифрования трафика между приложениями, в которых данный функционал не был реализован. Возможна работа в режиме клиента и сервера. Stunnel, работающий в режиме клиента, принимает незашифрованный трафик от некоего клиентского ПО по указанному ip-адресу и порту, затем зашифровывает и передаёт его на сервер. Если сервер поддерживает TLS (IIS, TrustedTLS и тд) – серверная часть stunnel’а не требуется. Применительно к задаче интеграции с сервисами Банка, нам потребуется настройка в режиме клиента.

В двух словах — это программа, на которую можно переложить всю логику шифрования трафика между сервером и клиентом. Утилита Stunnel позволит наиболее быстро обеспечить защищенный канал между клиентской частью, не поддерживающей ГОСТ алгоритмы и серверной частью Банка.

**2. Получение дистрибутива**

Глобально, есть 2 реализации этой утилиты, оригинальная версия stunnel, и версия stunnel-msspi. Оригинальная реализация stunnel при установке защищённых TLS-соединений использует библиотеку OpenSSL, которая ограниченно поддерживает криптографические алгоритмы ГОСТ. Для обеспечения работы ГОСТ-алгоритмов в полном объёме в stunnel-msspi используется интерфейс msspi , который поддерживает ГОСТ-алгоритмы, используя установленный в систему криптопровайдер. Внесение функционала msspi в проект stunnel сделано таким образом, что дополнены только участки кода связанные с интерфейсом OpenSSL , а проект в целом не претерпел существенных изменений.

В рамках тестирования для задачи поднятия канала, защищенного ГОСТ алгоритмами шифрования, подойдет любой вариант дистрибутива.

stunnel.win32.exe – версия дистрибутива для 32-битных ОС Windows, работает также в 64 битной версии, позволяет настроить запуск в качестве службы, но есть некоторые проблемы с перезапуском и стабильностью работы службы

stunnel.x64.exe – версия дистрибутива для 64-битных ОС Windows, возможна установка в качестве службы, но работа в качестве службы нестабильна, стабильная работа замечена только в консольном режиме.

stunnel\_msspi\_cli.exe – версия дистрибутива с поддержкой интерфейса msspi, работает только в консольном режиме, есть возможность указывать отпечаток сертификата вместо ссылки на файл.

stunnel\_msspi.exe – версия дистрибутива с поддержкой интерфейса msspi, работает и в качестве службы, и в консольном режиме, есть возможность указывать отпечаток сертификата вместо ссылки на файл. Для корректной работы в качестве службы необходима установка контейнера в раздел «Компьютер»

Обратите внимание, что stunnel-msspi входит в состав поставки, начиная с версии CSP 5.0 R2, поэтому версия stunnel-msspi в составе дистрибутива CSP будет сертифицирована.

Версия на github остаётся НЕ сертифицированной, она предполагает использование в тестовых и исследовательских целях.

**3. Установка и настройка утилиты stunnel**

Установка утилиты заключается в выполнении одной команды, которая выполнит установку исполняемого файла в качестве службы. Прежде чем выполнять установку утилиты, необходимо подготовить конфигурационный файл настроек stunnel.conf.

Вот готовый пример файла настроек:

output=d:\Stunnel\log\stunnel\_cli2.log

debug = 7

[https]

msspi = yes

client = yes

accept = 1543

connect = apiwsgdev.alfabank.ru:443

cert = 18f5e4fb7d9d62e03417130a667890cbfb45f144

verify = 2

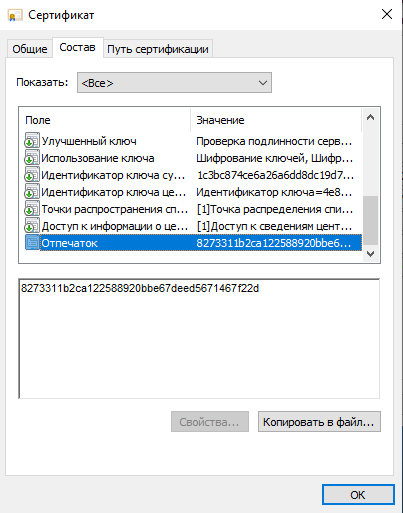
Client — указатель на то, является ли программа сервером или клиентом;

Accept — локальный порт, к которому будет подключаться программа;

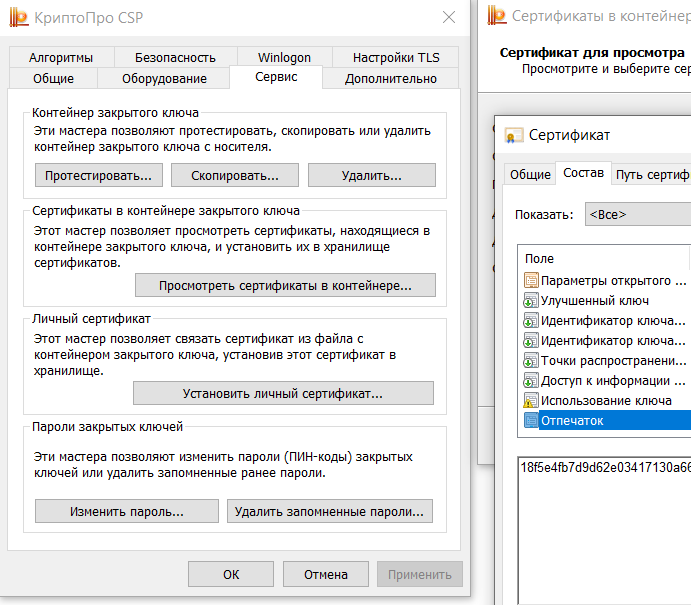
Connect — IP-адрес и порт сервера, с которым мы будем соединяться;

Verify — параметры:   
0. Не проверять сертификат сервера   
1. Проверять сертификат при его наличии   
2. Проверять сертификат всегда   
3. Проверять наличие данного сертификата в хранилище TrustedUsers

Cert — клиентский сертификат. Можно указать параметр двумя способами: либо импортировать сертификат из контейнера и прописать путь к файлу, либо воспользоваться отпечатком сертификата:

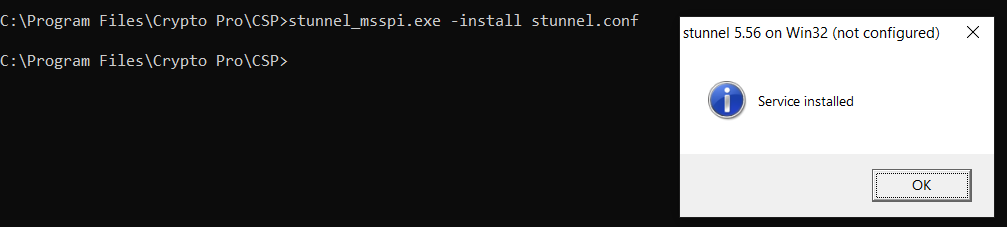


Посмотреть сертификат можно через приложение Crypto CSP:

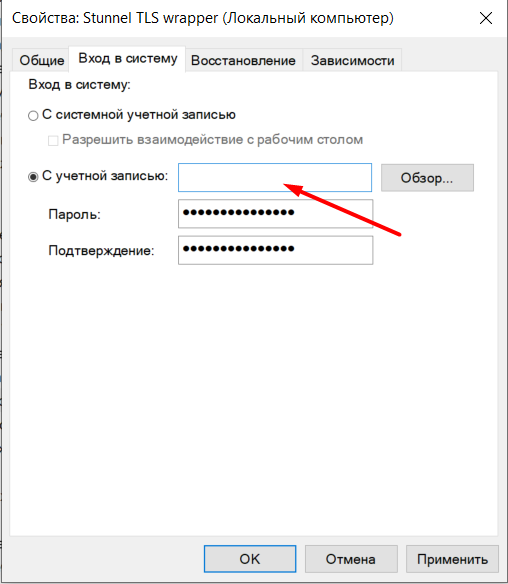


После того, как выполнена подготовка конфигурационного файла, выполняем установку командой из директории, где расположен конфигурационный файл командой:

stunnel\_msspi.exe -install stunnel.conf



Далее, необходимо будет в системе зайти в Панель управления\Все элементы панели управления\Администрирование, далее выбрать Службы. В службах найти службу Stunnel TLS wrapper и в разделе вход в систему прописать ту учетную запись, под которой будет стартовать служба:



Для старта сервиса выполняем команду C:\Program Files\Crypto Pro\CSP>stunnel\_msspi.exe -start

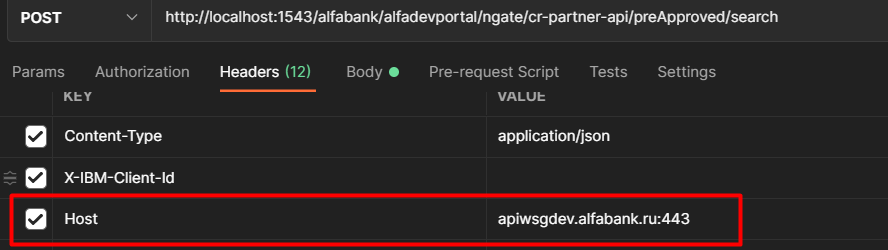
**4. Тестирование работоспособности**

Теперь все приложения на Windows станции смогут выполнить передачу по защищенному ГОСТ каналу без доработок. Для того, чтобы выполнить передачу по защищенному каналу, вам теперь нужно обращаться не на внешний адрес, а на локальный адрес станции и порт, прописанный в конфигурационном файле, в данном случае, 1543.

Для примера, приведен вызов из программы Postman для одного из сервисов. Приложение находится в режиме разработки, для промышленного режима предусмотрен другой эндпоинт

Обращаться будем по http на локалхост: <http://localhost:1543>

Важное замечание, обязательно явно укажите заголовок Host с адресом целевого хоста:



В остальном заголовки будут те же, ка и при прямом вызове.

