# Описание работы утилиты stunnel в режиме клиента на Windows 10 и режиме сервера на MAC OS X

В данном документе описан процесс подготовки к работе и функционирования утилиты stunnel в режиме клиента в среде ОС Windows 10 и режиме сервера в среде OS X El Capitan.

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. В режиме сервера stunnel принимает на заранее определённый в конфигурационном файле ip-адрес и порт зашифрованный трафик, затем расшифровывает его и передает соответствующему ПО на сервере.

В имеющемся в Mac OS X веб-сервере apache по умолчанию отсутствует функционал, реализующий соединение, зашифрованное по алгоритмам ГОСТ. Для обхода данного ограничения организуется работа утилиты stunnel в режиме сервера. Шифрованный трафик, приходящий на заранее указанный порт, будет расшифрован и направлен в открытом виде на порт, выделенный для Apache по умолчанию.

На Windows 10 утилита stunnel настроена в режиме клиента. Незашифрованный трафик поступает на заранее выбранный порт, затем шифруется и передаётся на указанный порт компьютера с Mac OS X и серверной частью stunnel.

В данном примере доступ осуществляется по конкретному сертификату клиента, присутствующему в хранилище TrustedUsers на сервере. Для выпуска сертификатов используется тестовый УЦ ООО "КРИПТО-ПРО" <u>https://www.cryptopro.ru/certsrv/</u>Возможны варианты, когда проверка сертификата производится только при его наличии, либо не производится вовсе - условия задаются опцией verify в конфигурационном файле stunnel.conf.

### Настройка клиентской части stunnel в среде Windows 10

Для работы в клиентском режиме потребуется установленное ПО КриптоПро CSP с действующей лицензией, сконфигурированная утилита stunnel, а также клиентский сертификат с объектным идентификатором в области использования ключа "проверка подлинности клиента"

После скачивания дистрибутива КриптоПро CSP с официального сайта и его последующей установки стандартным способом, производится выпуск клиентского сертификата. Сам сертификат может быть выпущен различными способами, но в рассматриваемом примере будет использоваться интерфейс тестового Удостоверяющего Центра ООО "КРИПТО-ПРО" https://www.cryptopro.ru/certsrv.

X 🟠 🏠 😳 https://www.cryptopro.ru/certsrv/ Ѻ ▾ 🚔 Ĉ 🖛 Тестовый Удостоверяющ... × » Центр реализован на основе службы сертификации, входящей в состав операционной системы Microsoft Windows Server 2012 R2. » Если вы используете веб-браузер, отличный от Microsoft Internet Explorer, то для получения сертификата нужно дополнительно установить КриптоПро ЭЦП Browser plug-in. Центр предназначен только для целей тестирования и не должен использоваться для других целей Центр не проверяет информацию, указанную в запросах на сертификат. Не следует доверять сертификатам, выданным тестовым Удостоверяющим Центром Узнать об услугах действующего Удостоверяющего Центра ООО "КРИПТО-ПРО" можно Получить сертификат Выберите нужное действие: > Сформ рос на сертификат » Отправить готовый запрос РКСS#10 или РКСS#7 в кодировке Base64 » Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификато © ООО "КРИПТО-ПРО", 2000-2015 0 へ 町 d)) 同 EN 

Далее отображен процесс скачивания корневого сертификата удостоверяющего центра и установки его в хранилище "Доверенные корневые центры сертификации".

Этот сертификат предназначается для: • Все политики выдачи • Все политики приченения • Все политики сертификатов ца	🔒 Сведения о сертификате	Службы сертификации Active Directory ( <i>Microsoft</i> ) — CRYPTO-PRO Test Center 2
Кому выдан:       СКИРТО-РКО Test Center 2         Кем выдан:       СКИРТО-РКО Test Center 2         Действителен с 05.08.2014 по 05.08.2019       Метод шифрования:         Установить сертификат       Завяление поставщика         Установить сертификат       Завяление поставщика	от сертификат предназначается для: • Все политном выдачи • Все политном применения	<ul> <li>Загрузка сертификата ЦС, цепочки сертификатов или CRL</li> <li>Чтобы доверять сертификатам, выданным этим центром сертификации, установите эту цепочку серти Чтобы загрузить сертификат ЦС, цепочку сертификатов или список отзыва сертификатов (CRL), выбе метод шифрования.</li> </ul>
Установить сертификат Заявление поставщика Загрузка сертификата ЦС Загрузка целочки сертификатов ЦС Загрузка последнего базового CRL	ону выдан: CRYPTO-PRO Test Center 2 ен выдан: CRYPTO-PRO Test Center 2 действителен с 05.08.2014 по 05.08.2019	— Сертификат ЦС: Терущий (СКҮРТО-РКО Test Center 2] Метод шифрования: ● DER
OK	Установить сертификат Заявление поставщие	Вазе 64     Загрузка сортификата ЦС     Загрузка цепочки сертификатов ЦС     Загрузка последнего базового CRL  ж

🔓 🈸 Мастер импорта сертификатов	Х s://www.cryptopro.ru/certsrv/certcarc.asp $\mathcal{P} \leftarrow \widehat{\blacksquare} \ \mathcal{C}$ → Службы сертификации Ас Х waции Active Directory ( <i>Microsoft</i> ) — CRYPTO-PRO Test Center 2
Хранилища сертификатов Хранилица сертификатов - это системные области, в которых хранятся сертификаты.	ификата ЦС, цепочки сертификатов или CRL
Windows автонатически выберет хранилище, или вы можете указать расположение сертификата врученую. О Автоматически выбрать хранилище на основе типа сертификата Понестить все сертификаты в следующее хранилище Хранилище сертификатов: Сбзор	Выбор хранилища сертификата с выбор хранилища сертификатов, которое вы с отите использовать.
Далее Отм	223

При выпуске сертификата клиента необходимо выбрать тип "Сертификат проверки подлинности клиента"

		0.4
	Intersection of the sector of	Службы сертификации Ас ×
	Province during clubic distance ru	
	Shekiponnazinovra. stumer_cient@stumer.ru	
	Opraнизация: stunnel_client	
	Подразделение: stunnel_client	
	Город: stunnel_client	
	Область, штат: stunnel_client	
	Страна, регион: RU	
CSPSetup	Тип требуемого сертификата:	
	Сертификат проверки подлинности клиента 🗸	
	Параметры ключа:	
	Создать новый набор ключей Оиспользовать	сушествующий набор ключей
	CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service	Provider V
	Использование ключей: О Еусбаров О Поллись О Оба	
	Размер клюца: 512 Минимальный:512 (стандартные размеры клюцей: 512	
	Паксимальный:512	
	Автоматическое имя контейнера ключа Зада Помотить ключ как экспортируемый	нное пользователем имя контеинера ключа
	Сохраняет сертификат в локальном хранилище компьютера	для сертификата е
	вместо пользовательского хранилища сертиф	икатов.
	Необходимо быть администратором, чтобы со	здать
	локальное хранилище.	
	Дополнительные параметры:	1
	Формат запроса: ОСМС • РКСS10	
	Алгоритм хеширования: ГОСТ Р 34.11-94 🗸	
	Используется только для подписания запроса.	
	Сохранить запрос	

При необходимости задаётся пароль на контейнер.

	Image: Comparison of the second s
	Параметры ключа:
	Создать новый набор ключей ОИспользовать существующий набор ключей
	Криптої Іро СSP × Service Provider × Использов Р Задайте пароль для создаваемого контейнера "te- 269103а9-0997-наfа-а126-7dc3aeb609c9".
	© Установить новый пароль EN Новый пароль EN
X	иотера для сертификата Подтверждение: вртификатов.
	локальное хранилище.
	Алгоритм хеширования: ГОСТ Р 34.11-94 У Используется только для подписания запроса.
	Атрибуты:
	Понятное имя:
	Выдать >

Производится установка сертификата.

	(a) ttps://www.cryptopro.ru/certsrv/certfnsh.asp	🔎 – 🔒 🖒 🍋 Службы се
k	Службы сертификации Active Directory ( <i>Microsoft</i> ) - CRYPTO	-PRO Test Center 2
	Сертификат выдан	
	Запрошенный вами сертификат был вам выдан.	
	Установить этот сертификат	
	□Сохранить ответ	

Создаётся рабочая папка, в которую производится экспорт созданного сертификата, а также копирование утилиты stunnel версии, соответствующей разрядности операционной системы (https://www.cryptopro.ru/products/other/stunnel).



В папке C:\Windows\system32 формируется файл конфигурации stunnel.conf

Galon       Главная       Поделиться       Вид         Закрепить на панели Колировать Вставить       Image: Construction of the second of the secon	🔜   🛃 🗖 =   System32			- 🗆	×
Bixperiume на панели Колировать Вставить       Repencerume в Хдалить *       Paenuto         Bixperiume на панели Колировать Вставить       Konuposati       Stonuposati       Stonuposati         Bixperiume на панели Колировать Вставить       Konuposati       Stonuposati       Stonuposati       Stonuposati         Bixperiume has namenu Konuposatis       Bixperiume has namenu Konuposatis       Stonuposatis       Stonuposatis       Stonuposatis         Bixperiume has namenu Konuposatis       StoreAgent.dll       StoreAgent.dll       StoreAgent.dll       StoreAgent.dll         Ackymental       StoreAgent.dll       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll         Bixperiume       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll         Bixperiume       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll       StoreVoc.dll         Bixperiume       Studeli       Studeli       Studeli       Studeli       Studeli       Studeli         Bixperiume       Studeli       Studeli       Studeli       Studeli       KS       KS         Cers       Studeli       Studeli       Studeli       Studeli       KS       KS         Cers       Studestatit       Studeli       St	Файл Главная Поделит	ться Вид			~ 😲
Быстрого доступа       Image: Non-point of the subscription difference of the subscription Mgr.dll         Буфер обмена       Image: Non-point of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription Mgr.dll       Image: Non-point Kommerce of the subscription Mgr.dll         Image: Non-point Kommerce of the subscription M	🖈 📑	Гаремести Вставить — Перемести	ить в т 🗙 Удалить т 🚺 🏪 🖓 💽 т	Паелить	
<ul> <li>← → · ↑  · ↑  · ↑  · ↑  · ↑  · ↑  · ↑  ·</li></ul>	быстрого доступа Буфер обмена		🥘 stunnel.conf — Блокнот — 🗆 义 Файл Правка Формат Вид Справка	< [+	
Pa6oчий сто.       Имя         Эагрузки       StoreAgent.dll         Эагрузки       StoreAgent.dll         Эагрузки       StoreAgent.dll         Эагрузки       StoreAgent.dll         Эагрузки       StoreAgent.dll         Эагрузки       StoreAgent.dll         Элементы       StoreAgent.dll         StoreAgent.dll       [https]         StoreAgent.dll       [https]         StoreAgent.dll       StoreAgent.dll         StoreAgent.dll       StoreAgent.dlll         StoreAgent.dlll       <	← → ~ ↑ <mark> </mark> « Локал	ьный диск (C:) > Windows >	output=c:\stunnel\stunnel.log	~	Q
→ Загрузки        StoreAgent.dll        debug = 7         [https]        3 K5             → Документы        Storevuauth.dll        [https]        6 K5             → Изображени        Storpop.dll        6 K5        7 K5             → StorSvc.dll        StorSvc.dll        connect = mac-admin:1502        5 K5             → Mysbika           → SturcturedQuery.dll        verify=2        5 K5             → Mysbika           → SubRange.uce           → SubRange.uce           → SubRange.uce           → K5             → Cerb           → Subst.exe           → Subst.exe           → K5           → K5             → Cerb           → Subst.exe           → Subst.exe           → K5           → K5             → Cerb           → Subst.exe           → Subst.exe           → K5           → K5             → Cerb           ⊕ Subst.exe           ⊕ Subst.exe           ↓ K5           ↓ K5             → Cerb           ⊕ SubfpaH 1 элементт: 216 байт	🔜 Рабочий сто. 🖈 ^ – V	1мя ^	<pre>socket = 1:TCP_NODELAY=1 socket = r:TCP_NODELAY=1</pre>		^
Документы Storewuauth.dll   Msoбражени Storpop.dll   Storpop.dll Storpop.dll   Mysbika Streamci.dll   SubRange.uce SubscriptionMgr.dll   SubscriptionMgr.dll Storpop.dll   SubscriptionMgr.dll Storpop.dll   SubscriptionMgr.dll Kb   Sublesp.dll Kb   Sublesp.dll Kb   Sublesp.dll Kb	👆 Загрузки 🖈 🛛	StoreAgent.dll	debug = 7	3 KE	
Image: Moofpaxeerux Storprop.dll accept=192.168.198.128:1555 7 KB   Image: stunnel StorSvc.dll cert=0:168.198.128:1555 5 KB   Image: stunnel Streamci.dll cert=0:15tunnel_client.cer 7 KB   Image: stunnel.conf SubscriptionMgr.dll 1 KB   Image: stunnel SubscriptionMgr.dll 9 KB   Image: stunnel SubscriptionMgr.dll 9 KB   Image: stunel SubscriptionMgr.dll 9 KB   Image: stunel SubscriptionMgr.dll 1 KB   Image: stunel SubscriptionMgr.dll 9 KB   Image: stunel SubscriptionMgr.dll 1 KB   Image: stude stude SubscriptionMgr.dll 9 KB   Image: stude st	🔮 Документы 🖈	🗟 storewuauth.dll	[https]	6 KE	
Stunnel       StorSvc.dll	📰 Изображени 🖈	Storprop.dll	accept=192.168.198.128:1555	7 КБ	
Видео       streamci.dll       cert=C:\stunnel_client.cer       7 КБ         Музыка       stunel.conf       5 KБ         OneDrive       SubRange.uce       2 КБ         Этот компьютер       subst.exe       9 КБ         Этот компьютер       subst.exe       6 КБ         SubcriptionMgr.dll       1 КБ       1 КБ         Элементов: 3 732       Выбран 1 элемент: 216 байт       с	stunnel	StorSvc.dll	connect = mac-admin:1502	5 KE	
Музыка       StructuredQuery.dll       verify=2       5 КБ         Музыка       Stunnel.conf       1 КБ         OneDrive       SubRange.uce       2 КБ         Этот компьютер       subst.exe       9 КБ         Этот компьютер       subst.exe       6 КБ         Sublesp.dll       1 КБ         У П СилбасыШикЦинациет dll       7 ИС         Элементов: 3 732       Выбран 1 элемент: 216 байт	Вилео	🗟 streamci.dll	<pre>cert=C:\stunnel\stunnel_client.cer</pre>	7 КБ	
<ul> <li>Inivisibilità</li> <li>SubRange.uce</li> <li>SubRange.uce</li> <li>SubscriptionMgr.dll</li> <li>Этот компьютер</li> <li>subst.exe</li> <li>Suplcsps.dll</li> <li>Suplcsps.dll</li></ul>	видео	StructuredQuery.dll	verify=2	5 KE	
Image: SubRange.uce       2 КБ         Image: SubRange.uce       9 КБ         Image: SubScriptionMgr.dll       9 КБ         Image: SubStription Mgr.dll       6 КБ         Image: SubStription Mgr.dll       1 КБ         Image: SubStription Mgr.dll       4 КБ         Image: SubStription Mgr.dll       7 VE	л музыка	stunnel.conf		1 КБ	
Этот компьютер         9 КБ           Этот компьютер         6 КБ                Сеть          SubscriptionMgr.dll                 У Сеть          SubscriptionMgr.dll                 У Сеть          SubscriptionMgr.dll                 У Сеть          Suplcsps.dll                 У Посторытьющие и          4 КБ                 У посторытьющие и          7 кс	la OneDrive	SubRange.uce		2 КБ	
<ul> <li>Этот компьютер</li> <li>© subst.exe</li> <li>© sud.dll</li> <li>© Suplesps.dll</li> <li>Элементов: 3 732</li> <li>Выбран 1 элемент: 216 байт</li> </ul>		SubscriptionMgr.dll		9 KE	
<ul> <li></li></ul>	🛄 Этот компьютер	📧 subst.exe		6 KE	
<ul> <li>Зирісярь.dll</li> <li>Элементов: 3 732</li> <li>Выбран 1 элемент: 216 байт</li> </ul>	🔿 Сеть	🖄 sud.dll		1 KE	
Злементов: 3 732 Выбран 1 элемент: 216 байт		🖄 Supicsps.dli		4 KE	~
	Элементов: 3 732 Выбран 1	லி Curfaca⊔ub⊔andlere dli алемент: 216 байт	< > > >	TVE	
	Solution of the Deloper 1.	Shewenn Ero oom		412	

Содержимое конфигурационного файла stunnel.conf клиентской части:

output=C:\stunnel\stunnel.log socket=I:TCP\_NODELAY=1 socket=r:TCP\_NODELAY=1 debug=7 [https] Accept=192.168.198.128:1555 Connect=mac-admin:80 Cert= C:\stunnel\stunnel\_client.cer

Verify=2

Краткое описание наиболее часто используемых параметров конфигурации.

Опция	Описание	
Pid (в unix	Путь к файлу, в котором будет храниться идентификатор процесса	
системах)		
output	Путь к лог-файлу	
socket	Опции для конфигурирования принимающих, локальных, удалённых	
	сокетов.	
debug	Уровень протоколирования (для экономии места на диске	
	рекомендуется устанавливать значение 1)	
client	Работа в режиме клиента	
accept	Адрес и порт для приёма незашифрованного трафика	
connect	Адрес и порт сервера, на который передаётся зашифрованный трафик	
cert	Путь к файлу сертификата клиента	
verify	Возможные варианты проверки сертификата удалённого сервера	
	0. Не проверять сертификат сервера	
	1. Проверять сертификат при его наличии	
	2. Проверять сертификат всегда	
	3. Проверять наличие данного сертификата в хранилище	
	TrustedUsers	
pincode	PIN-код контейнера	

Далее в командной строке, запущенной с правами администратора, производится установка службы stunnel, после чего в оснастке services.msc указывается учётная запись, под которой будет работать служба. Производится запуск самой службы.

Администратор: Ког	мандная строка	- U X		
Microsoft Windows [Versi (с) Корпорация Майкрософ	ion 10.0.10240] þī (Microsoft Corporation), 2015 г. Вс	е права защищены.		
C:\WINDOWS\system32>c:\s Stunnel Service installe	stunnel\stunnel.exe -install ed.			
:\WINDOWS\system32>				
			Свойства: Stunnel Servic	е (Локальный компьютер)
	Stumerservice	v ^	Общие Вход в систему	Восстановление Зависим
		BranchCache	Вход в систему:	
	Запустить службу	CDPSvc	ОС системной учетно	й записью
		CoreMessaging	Разрешить взаим	иодействие с рабочим столом
		Q DataCollectionPu		NIL222
		🥘 DHCP-клиент	• С учетной записью:	.\User
		🧟 dmwappushsvc	Пароль:	•••••
		🔍 DNS-клиент	Поотроница	
		embeddedmode	подтверждение.	
		🔐 Enterprise App M		
		🔐 KtmRm для коор		
		Plug and Play		
		Quality Windows		
		SIVIP дисковых пр		
		Superfetch		
		TP AutoConnect		
		Autoconnect		

При наличии PIN на контейнере потребуется, либо сохранить его в памяти средствами CSP(протестировать контейнер, поставив галку "запомнить пароль"), или указать в явном виде в файле конфигурации, использовав опцию pincode.

## Настройка серверной части stunnel в среде Mac OS X

Производится запуск имеющегося в системе веб-сервера Apache. Используется команда sudo apachectl start



Утилита stunnel входит в дистрибутив КриптоПро CSP для MAC OS X и должна быть выбрана для установки вместе с остальными пакетами.



Завершив установку, можно проверить содержимое папки /opt/cprocsp/sbin



Далее будет установлен корневой сертификат удостоверяющего центра, а также произведён выпуск сертификата сервера. Для работы с интерфейсом тестового удостоверяющего центра (т.к. генерация контейнера будет производиться в хранилище компьютера, а не пользователя) понадобится запустить браузер Safari с правами администратора. Для этого используется команда: sudo open /Applications/Safari.app



Необходимо скачать и установить корневой сертификат тестового УЦ ООО "КРИПТО-ПРО" на котором будет произведён выпуск сертификата сервера.



Установка производится командой ./certmgr –inst –store –root –f /Users/admin/Downloads/certnew.cer



Далее средствами тестового УЦ ООО "КРИПТО-ПРО" производится выпуск сертификата с типом "проверка подлинности сервера". Ключевым моментном здесь является соответствие значения поля "Имя" имени самого сервера(hostname).

Satari Файл Правка	Вид История Закладки Window Справка	())) 🛲 (
	🗎 cryptopro.ru 🔿	0 1
00 @	Спужбы сертификации Active Directory ( <i>Microsoft</i> ) - CRYPTO-PRO Test Center 2	Дс
Q. Поиск в заклавках	Расширенный запрос сертификата	
▶ ☆ Избранное	Идентифицирующие сведения:	
	Имя: mac-admin	
	Электронная почта: mac-admin	
	Oprahusauus: mac-admin	
	Подразделение: mac-admin	
	FODOR: mas-admin	
	Область штат: mac-admin	
	Страна, регион: RU	
	Тип требуемого сертификата:	
	Сертификат проверки подлинности сервера 📀	
	Параметры ключа:	
	Создать новый набор ключей Использовать существующий набор ключей	
	CSP: Crypto-Pro GOST R 34.10-2001 KC1 CSP	
	Использование ключей: ОЕхсhange ОПодпись ООба	
	Размер ключа: 512 Минимальный:512 (стандартные размеры ключей: 512.)	
	Автоматическое имя контейнера ключа Заданное пользователем имя контейнера	слюча
	Пометить ключ как экспортируемый	
	Использовать локальное хранилище компьютера для сертификата Сохраняет сертификата в покальном хранилице сертификатов. На устанаелизает колономисти и собранилице сертификатов. На устанаелизает корневої сертификат ЦС. Наобходимо быть администратором, чтобы создать покатиче з такищине.	
Правка		
	Дополнительные параметры:	
	) 💋 📉 📕 🔟 🚺 📒 🍪 🕖 💋 🚫 🙆 🗀 📢	

Производится генерация контейнера и задается PIN.

$\bullet \bullet \bullet < > \square$	i cryptopro.ru C	0
	жбы сертификации Active Directory ( <i>Microsoft</i> ) CRYPTO-PRO Test Center 2	
Q. Поиск в закладках	тификат выдан	
▶☆ Избранное 3	рошенный вами сертификат был вам выдан.	
	Установить этот сертификат	
	Сохранить ответ	
	CryptoPro CSP Type password for container "389/5132f-70ab-df94-39dc-c7e10110108"	
	Password:	
	Cancel	
Правка		
	) 🔝 💼 📆 📁 🔝 🎧 🍙 🕼 🔚 🥌 🗎	

Проверить наличие сертификата в хранилище "Личное" можно, используя команду:

#### ./certmgr –list –store mmy

		🔒 cryptopro.ru	C
		🛅 bin — -bash — 133×45	
Mac-Admin:~ admin\$ Mac-Admin:bin admin Certmgr 1.0 (debug C€ program for managin	<pre>cd /opt/cprocsp/bin/ \$ ./certmgr -list -store mm version) (c) "CryptoPro", g certificates, CRLs and st</pre>	y 2007-2010. ores	
1			
Techor	· E-support@cruptopro_ru	C-RU L-Moscow O-CRYPTO-RRO LLC (N-	CRYPTO_PRO Test Contes 7
Issuer Subject	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi	C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN= n, OU=mac-admin, O=mac-admin, L=mac-a	CRYPTO-PRO Test Center 2 admin, S=mac-admin, C=RU
Issuer Subject Serial	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi : 0x12000ADF5A06DCB6503A8C	C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN= n, OU=mac-admin, O=mac-admin, L=mac-a E2D700000000ADFSA	CRYPTO-PRO Test Center 2 Idmin, S=mac-admin, C=RU
Issuer Subject Serial SHA1 Hash SubiKeyTD	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi : 0x12000ADF5A060CB6503A8C : 0x9969f7dc3898044dc596db - 42cf07275d2b87013fo38148	C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN= n, OU=mac-admin, O=mac-admin, L=mac-a E2D70000000ADF5A 0272cd54b0c7d1e427 3baa36568715600	CRYPTO-PRO Test Center 2 dmin, S=mac-admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi : 0x12000ADF5A06DCB6503A8C : 0x9969f7dc3898bd4de596db : 42cf97275d2b97913fe281d8 : FOCT P 34.11/34.10-2001	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D70800000ADF5A 0272cd54b0c7d1e427 3baa365688716c00	CRYPTO-PRO Test Center 2 admin, S=mac-admin, C=RU
Issuer Subject Serial SHAI Hash SubjKeyID Signature Algorithm PublicKey Algorithm	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi : 0x12000ADF5A06DCB6503A8C : 0x9969f7dc3898bd4de596db : 42cf97275d2b97913fc281d8 : FOCT P 34.11/34.10-2001 : FOCT P 34.10-2001 (512 b	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D700000000ADF5A 0272cd54b0c7die427 3baa365688716c00 its)	:CRYPTO-PRO Test Center 2 dmin, S=mac-admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm PublicKey Algorithm Not valid before	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi 0x12000ADF5A66DC6503A8C : 0x9960f7dc3308b64dc6506d : 42cf9727532b97913fc281d8 : 70CT P 34.11/34.10-2001 : 70CT P 34.10-2001 (512 b : 26/11/2015 15:36:01 UTC	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D7080080ADF5A 8272cd54b0c7d1e427 3baa365688716c00 its)	:CRYPTO-PRO Test Center 2 dmin, S=mac-admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm PublicKey Algorithm Not valid before Not valid after	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi : 0x12000ADF5A66CE6503ABC : 0x9969f7dc3898bd4de596db : 42cf97275d2b97913fc281d8 : FOCT P 34.11734.10-2001 : FOCT P 34.119-2001 (512 b : 26/02/2016 15:46:01 UTC 26/02/2016 15:46:01 UTC	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D70800000ADF5A 0272cd54b0c7d1e427 3baa365688716c00 its)	:CRYPTO-PRO Test Center 2 dmin, S=mac-admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm PublicKey Algorithm Not valid before Not valid after PrivateKey Link	: E=support@cryptopro.ru; : E=mac-admin, CN=mac-admi 0x12000ADF5A60Cb6503ABC 0x9960f7dc3398bd4dc596db : 42cf9727d2398bd4dc596db : 42cf9727d2398bd4dc596db : 42cf97273d2997914784 : 70CT P 34.10-2001 : 70CT P	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D70000000ADF5A 8272cd54b0c7d1e427 3baa365688716c00 its)	CRYPTO-PRO Test Center 2 ¦dmin, S=mac−admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm PublicKey Algorithm Not valid before Not valid after PrivateKey Link Container	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi 0x12000ADF5A66Dc6503A8C : 0x9960f7dc3308b64dc6506db : 42cf97273d2b97913fc281d8 : FOCT P 34.11/34.10-2001 : FOCT P 34.10-2001 (512 b : 26/11/2015 15:36:01 UTC : 26/02/2016 15:46:01 UTC : Yes HDIMAGE\\ffe85151.000\02	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D7080080ADF5A 8272cd54b0c7d1e427 3baa365688716c00 its)	CRYPTO-PRO Test Center 2 dmin, S=mac−admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm Publickey Algorithm Not valid before Not valid after PrivateKey Link Container Provider Name	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi : 0x12000ADF5A66Cb6503ABC : 0x9969f7dc3898bd4de596db : 42cf97275d2b97913fc281d8 : FOCT P 34.1134.10-2001 : FOCT P 34.1134.10-2001 : COCT P 34.1124.10-2001 : 26/02/2016 15:36:01 UTC : Yes : HDIMAGE\\ffe85151.000\02 C rypto-Pro GOST R 34.10-	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D70800000ADF5A 0272cd54b0c7d1e427 3baa365688716c00 its) A1 2001 KC1 CSP	CRYPTO-PRO Test Center 2 √dmin, S=mac-admin, C=RU
Issuer Subject Serial SHA1 Hash SubjKeyID Signature Algorithm PublicKey Algorithm Not valid before Not valid after PrivateKey Link Container Provider Name Provider Info	: E=support@cryptopro.ru, : E=mac-admin, CN=mac-admi 0x12000ADF5A60EC6503ABC : 0x9960f7dc3898b44dc596db : 42cf97273d297914f281d8 : FOCT P 34.11/34.10-2001 : FOCT P 34.10-2001 (512 : 26/11/2015 15:36:01 UTC : 26/02/2016 15:46:01 UTC : Yes : HOIMAGE\\ffe85151.00\X2 : Crypto-Pro GOST R 34.10- ProvType: 75, KeySpec: 1	C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN= n, 0U=mac-admin, 0=mac-admin, L=mac-a E2D70800800ADF5A 0272cd54b0c7d1e427 3baa365688716c00 its) A1 2001 KC1 CSP , Flags: 0x20	:CRYPTO-PRO Test Center 2 dmin, S=mac-admin, C=RU

Далее следует определить рабочую папку утилиты и произвести в неё экспорт сертификата.

Exporting:	
1	
Issuer	: E=support@cryptopro.ru, C=RU, L=Moscow, 0=CRYPT0-PR0 LLC, CN=CRYPT0-PR0 Test Center
Subject	: E=mac-admin, CN=mac-admin, OU=mac-admin, O=mac-admin, L=mac-admin, S=mac-admin, C=RU
Serial	: 0x12000ADF5A06DCB6503A8CE2D70000000ADF5A
SHA1 Hash	: 0x9969f7dc3898bd4de596db0272cd54b0c7d1e427
SubjKeyID	: 42cf97275d2b97913fe281d83baa365688716c00
Signature Algorithm	: FOCT P 34.11/34.10-2001
PublicKey Algorithm	: FOCT P 34.10-2001 (512 bits)
Not valid before	: 26/11/2015 15:36:01 UTC
Not valid after	: 26/02/2016 15:46:01 UTC
PrivateKey Link	: Yes
Container	: HDIMAGE\\ffe85151.000\02A1
Provider Name	: Crypto-Pro GOST R 34.10-2001 KC1 CSP
Provider Info	: ProvType: 75, KeySpec: 1, Flags: 0x20
Extended Key Usage	: 1.3.6.1.5.5.7.3.1

В случае, если использование тестового УЦ не предполагается, а контейнер с сертификатом сервера получен ранее и присутствует на внешнем носителе – производится копирование контейнера в папку /var/opt/cprocsp/keys, после чего осуществляется установка сертификата. В зависимости от типа ключевого носителя механизм копирования контейнера может отличаться. В случае работы с флеш-картой осуществляется копирование папки [имя\_контейнера].000 в указанную выше директорию с помощью команды cp . Если же используется к примеру защищённый ключевой носитель Рутокен S, то сначала командой ./csptestf –keyset –enum\_cont –verifyc-fqcn проверяется наличие на нём контейнеров, а затем производится копирование нужного контейнера в хранилище локального компьютера. Для этого используется команда ./ csptest -keycopy -src '\\.\Aktiv Rutoken S 00 00\имя\_контейнера'-dest '\\\HDIMAGE\имя\_контейнера' –machinekeyset Установка сертификата производится командой ./csptestf -absorb -certs -machine Следующим шагом будет формирование конфигурационного файла stunnel.conf в рабочей папке программы (файл может быть сформирован в произвольном месте).



Содержимое конфигурационного файла stunnel.conf серверной части:

pid = /Users/admin/Documents/stunnel.pid

output=/Users/admin/Documents/stunnel.log

socket=I:TCP\_NODELAY=1

socket=r:TCP\_NODELAY=1

debug=7

[https]

Accept=192.168.198.129:1502

Connect=192.168.198.129:80

Cert=/Users/asdmin/Documents/mac-admin.crt

Verify=3

В данном примере показан случай, когда проверка клиента производится по конкретному сертификату (опция verify=3), который должен присутствовать в хранилище TrustedUsers сервера. Производится копирование сертификата на сервер, а затем установка в указанное хранилище. Сертификат устанавливается командой ./certmgr -inst -store TrustedUsers -f /Users/admin/Desktop/stunnel\_client.cer



🧯 Терминал	Shell Правка Вид Окно Справка
	📃 sbin — -bash — 80×27
[Mac-Admin:bin admi [Mac-Admin:sbin adm Mac-Admin:sbin adm	n\$ cd /opt/cprocsp/sbin/ ] in\$ ./stunnel_thread /Users/admin/Documents/stunnel.conf ] in\$ []
	CryptoPro CSP Type password for container "ffe851510-4caf-ff61-7297-c8020e1c762"
	Cancel OK

Производится запуск утилиты stunnel\_thread с указанием конфигурационного файла. Если присутствующий на контейнере PIN не указан в явном виде в файле конфигурации, отобразится окно с запросом ввода.

Далее необходимо проверить корректность работы. Для этого производится попытка доступа по соответствующему адресу http://192.168.198.128:1555 с клиентской машины.



#### Возможные ошибки в работе

В случае возникновения проблем с подключением следует изучить содержимое файла журнала событий, который создаётся автоматически при первом запуске службы по указанному в конфигурационном файле пути. При некорректно сформированном конфигурационном файле утилита не запустится, при этом файлы журнала и идентификатора процесса могут не создаваться.

- 1. Если в файле конфигурации PIN на контейнер указан с ошибкой служба запустится, но при попытке соединения клиента PIN будет запрошен вновь.
- 2. При настройке клиента на ОС следует удостовериться в корректности значения опции **accept**. При наличии ошибок в файле конфигурации запустить службу не удастся.

🛱 Службы Файл Действие Вид Справка		Службы			×	>	<
о 🗇 🌩 🕅 🖾 🤉	Image: CryxKbi (локальні           CryxKbi (локальні           Stunnel Service           Запустить службу	Служба "Stunnel Service" на "Локальный компьютер" была запущена и затем остановлена. Некоторые службы автоматически останавливаются, если они не используются другими службами или программами.		ески ми ОК	ска (ак	^	
	l		SMP дисковых пространст	Служба уз	Вручнук Вручнук	] 0 0	
			Superfetch	Поддержи Выполняется	Автомат	иче >	~
	Расширенный (Станла	ртный /					

3. При отсутствии в хранилище root корневого сертификата сервера(в случае, если

сертификаты сервера и клиента выпущены разными УЦ) к которому производится

подключение, в журнале событий отобразится сообщение следующего плана: Error 0x20 ((unknown)) returned by CertVerifyCertificateChainPolicy! Error 0x20 when validate certificate

```
Error 0x80092004 returned by VerifyCertChain
**** Error 0x80092004 authenticating server credentials!
Connection reset: 0 byte(s) sent to SSL, 0 byte(s) sent to socket
```

4. Если при использовании oпции verify=3 в xpанилище ceptuфикатов "TrustedUsers"

будет отсутствовать сертификат клиента – подключение не удастся, а в логах

```
отобразится ошибка.
:56:29 L0G7[32181:123145306087424]: <u>Recieve</u> 96 bytes from client on
                                                                                                                                 and
Loop
:56:29 L0G7[32181:123145306087424]: AcceptSecurityContext finish, <u>scRet</u>
                                                                                                                                 edUs
:56:29 L0G5[32181:123145306087424]: Send 1139 handshake bytes to client
:56:29 L0G7[32181:123145306087424]: reading in SSPINeg err = 890
:56:29 L0G7[32181:123145306087424]: <u>Recieve</u> 890 bytes from client on
:56:29 L0G7[32181:123145306087424]: AcceptSecurityContext finish, scRet
:56:29 L0G3[32181:123145306087424]: Error 0x80092004 returned by
ficateInStore "TrustedUsers"
:56:29 L0G5[32181:123145306087424]: User not authorized for connect
:56:29 L0G5[32181:123145306087424]: 11 bytes of close_notify data sent
:56:29 L0G5[32181:123145306087424]: Connection reset: 0 byte(s) sent to
                                                                                                                                 d
) sent to socket
:56:29 L0G7[32181:123145306087424]: free Buffers
:56:29 L067[32181:123145306087424]: free buffer
:56:29 L067[32181:123145306087424]: delete c=>hContext
:56:29 L065[32181:123145306087424]: incomp_mess = 0, extra_data = 0
:56:29 L067[32181:123145306087424]: Local socket (FD=4) closed
:56:29 L067[32181:123145306087424]: Service [https] finished (0 left)
:56:29 L067[32181:123145306087424]: str_stats: 7 block(s), 824 data
control buto(s)
control byte(s)
:56:29 L0G7[32181:123145306087424]: str stats: 128 byte(s) at
anches/CSP_4_0/CSPbuild/CSP/samples/stunnel/src/network.c:430
:56:29 L0G7[32181:123145306087424]: str_stats: 128 byte(s) at /
anches/CSP_4_0/CSPbuild/CSP/samples/stunnel/src/network.c:429
```