Руководство администратора сервера Транссиг-сервер

Оглавление

Аннотация

Программный продукт «Сервер электронной подписи Транссиг» («Транссиг-сервер») является приложением, реализующей передачу запросов от внешних к СКЗИ «Сигнатура».

Системные требования

Транссиг-сервер функционирует на компьютере под управлением ОС Windows версий 7, 8, 8.1, 10, а также Windows Server 2008 R2, 2012, 2012 R2, 2016 с установленным .Net Framework 4.6.2.

Установка приложения

Перед установкой Транссиг-сервера необходимо

-Установить .Net Framework 4.6.2;

-Установить СКЗИ СКАД Сигнатура;

-Установить СЗИ СКАД: Справочник сертификатов;

-Установить СКАД Сигнатура SDK;

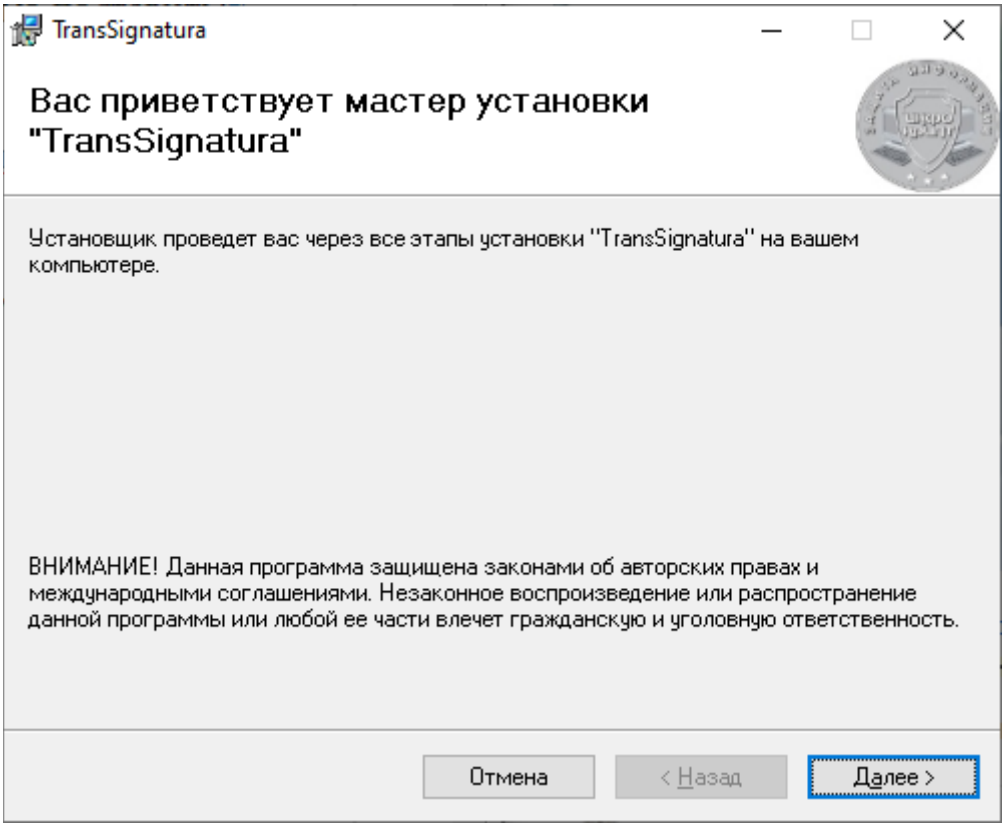
Если необходимо использовать логирование в oracle, то так же необходимо поставить:

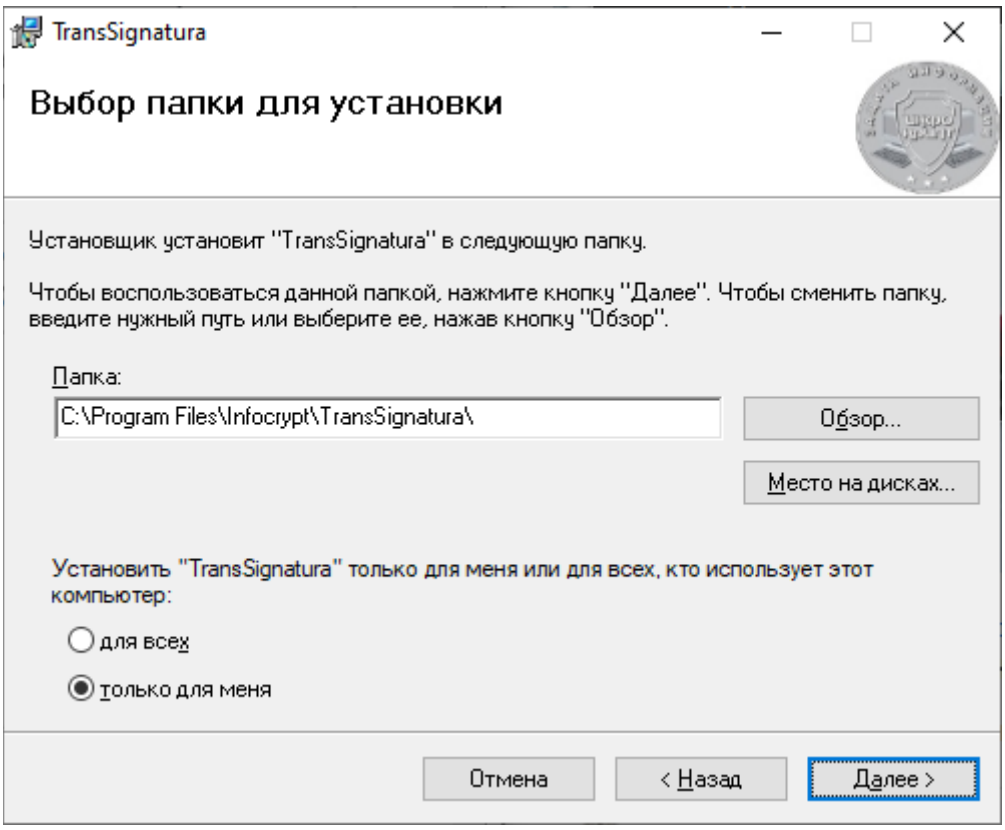
-Oracle Client

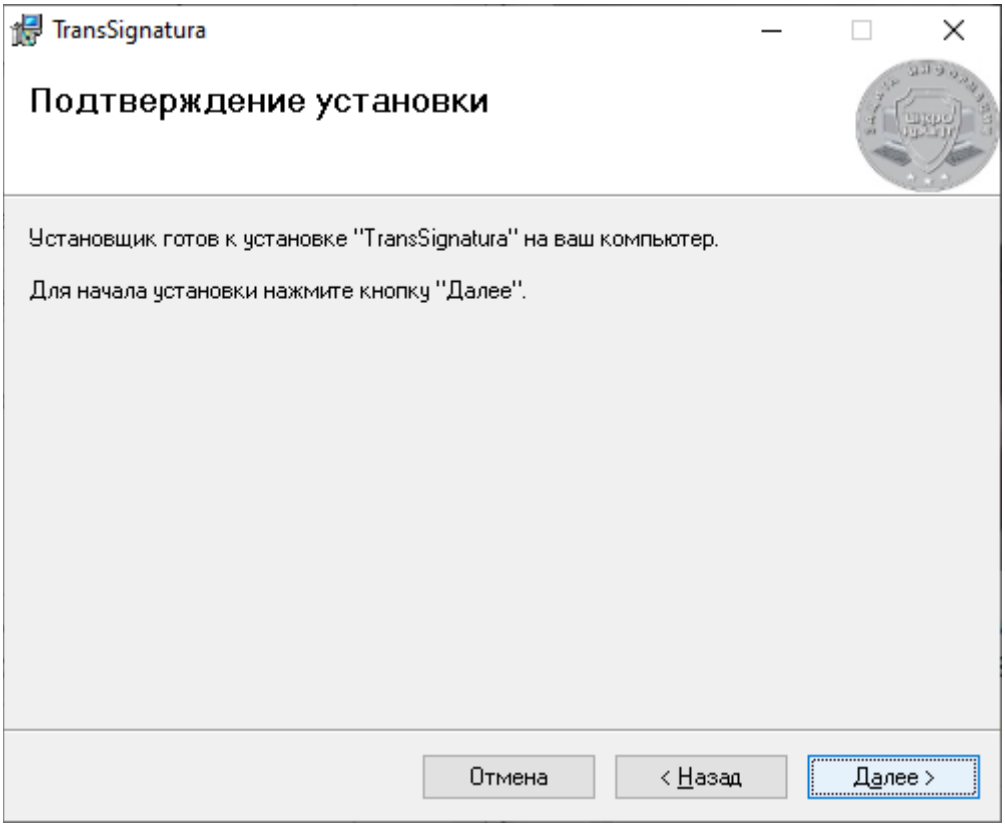
Если предполагается использовать защищенное хранилище ключей, то необходимо поставить

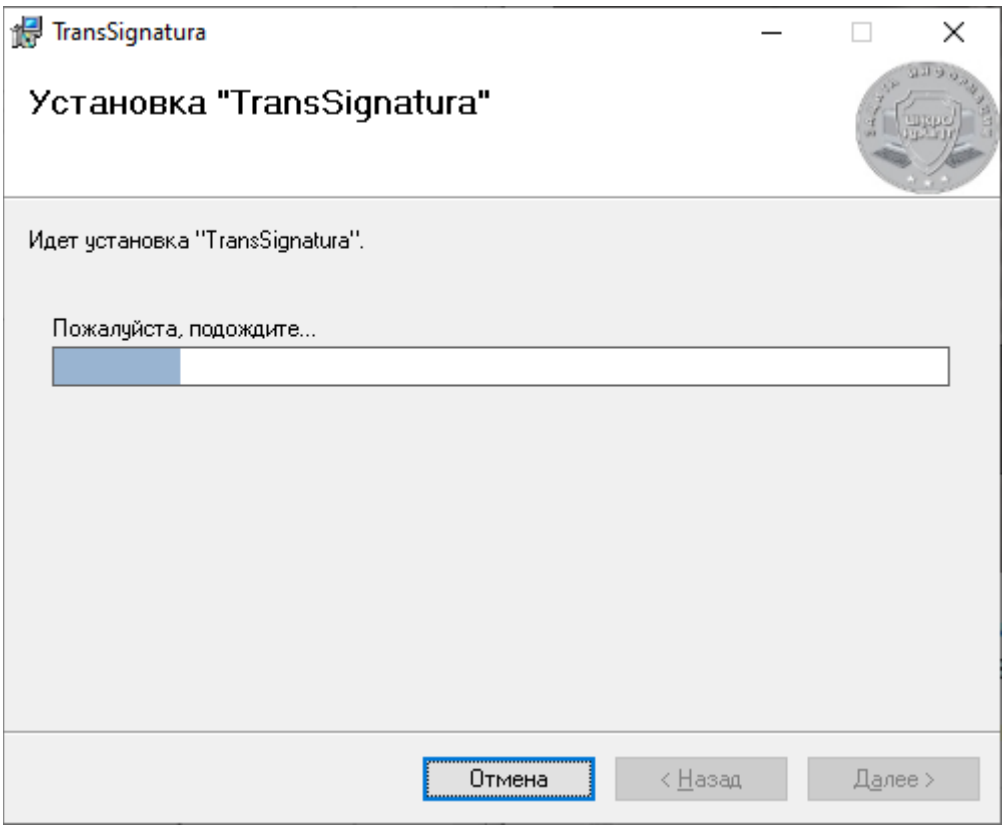
-ImDisk

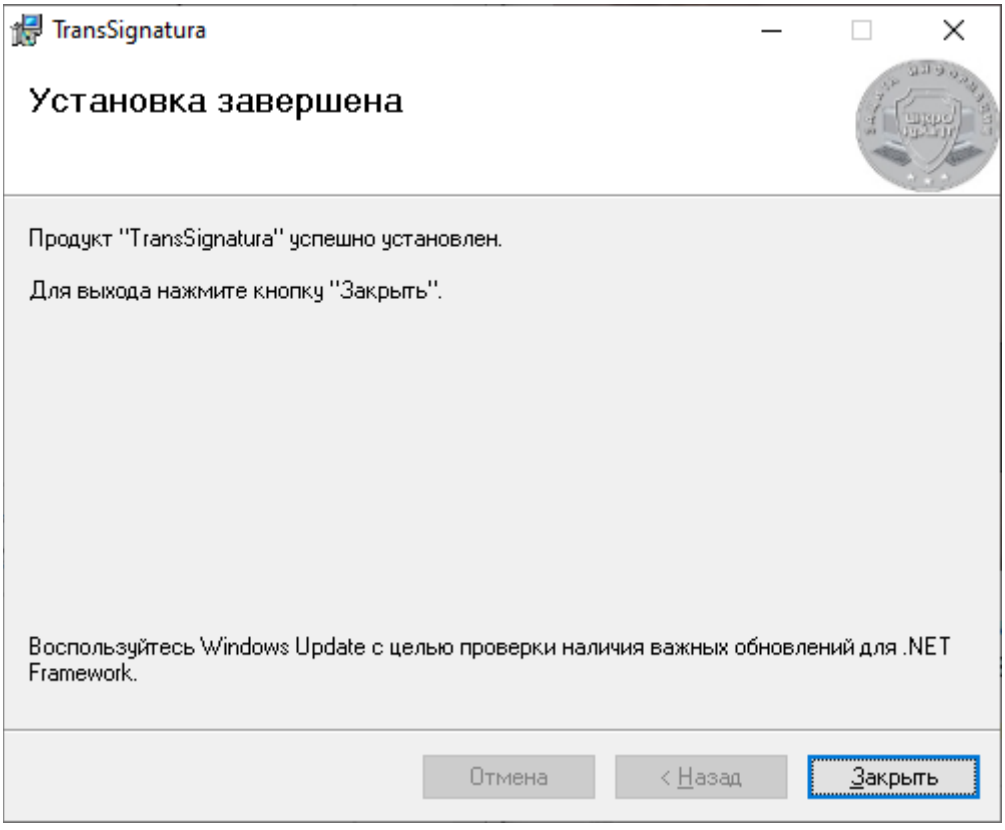
Сама установка происходит инсталлятором собранном на основе Windows Installer. Перед установкой новой версии обязательно необходимо удалить старую. Процесс установки отображен на снимках экрана ниже.




TransSignatura
Выбор папки для установки
Установщик установит "TransSignatura" в следующую папку.
Чтобы воспользоваться данной папкой, нажмите кнопку "Далее". Чтобы сменить папку, введите нужный путь или выберите ее, нажав кнопку "Обзор".
Папка:
C:\Program Files\Infocrypt\TransSignatura\
Обзор...
Место на дисках...
Установить "TransSignatura" только для меня или для всех, кто использует этот компьютер:
для всех
только для меня
Отмена
< Назад
Далее >


TransSignatura
Подтверждение установки
Установщик готов к установке "TransSignatura" на ваш компьютер.
Для начала установки нажмите кнопку "Далее".
Отмена
< Назад
Далее >


TransSignatura
Установка "TransSignatura"
Идет установка "TransSignatura".
Пожалуйста, подождите...
Отмена
< Назад
Далее >

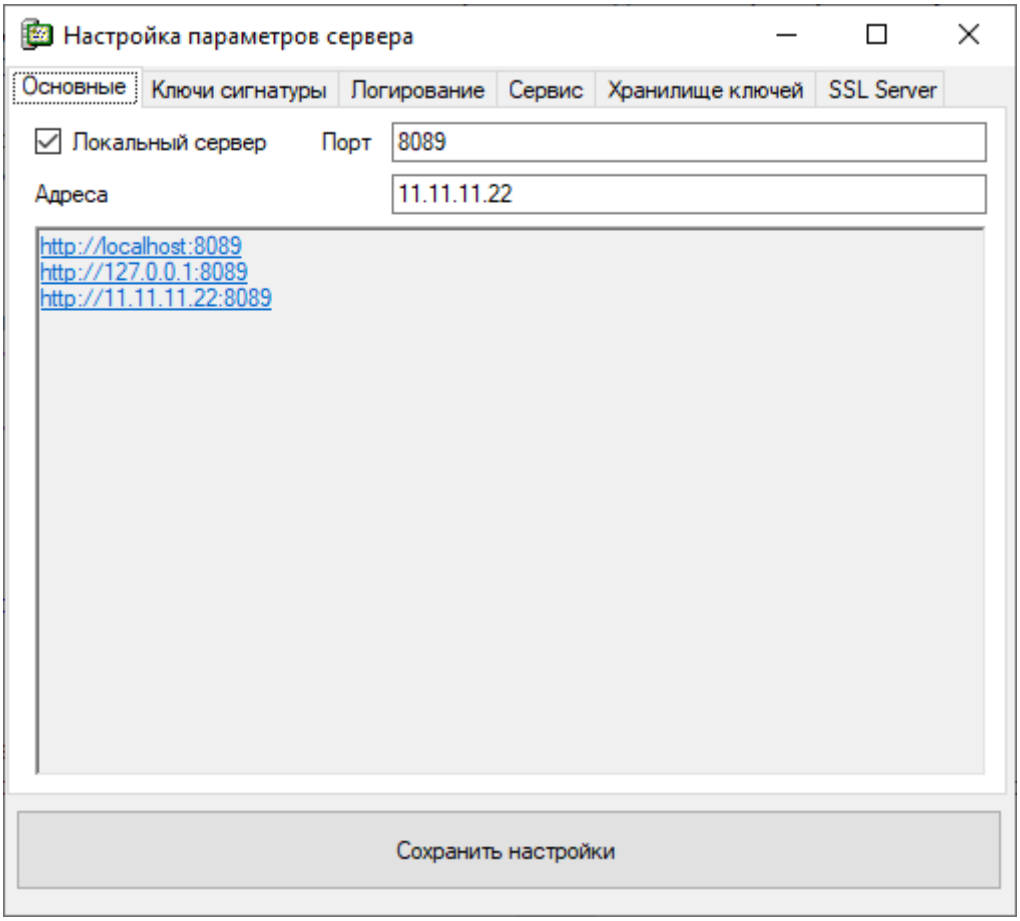

TransSignatura
Установка завершена
Продукт "TransSignatura" успешно установлен.
Для выхода нажмите кнопку "Закрыть".
Воспользуйтесь Windows Update с целью проверки наличия важных обновлений для .NET Framework.
Отмена
< Назад
Закрыть

Настройка приложения

Настройка Транссиг-Сервера происходит в специальном приложении. Сами настройки хранятся в файле transsignatura.config. Файл расположен в каталоге приложения и в каталоге пользователя \AppData\Local\. После изменения настроек, для их применения, необходимо нажать кнопку сохранить настройки и перезапустить приложение (или сервис).

Основные настройки

На этой вкладке необходимо указать адреса, которые Транссиг-Сервер, будет использовать для прослушивания входящих соединений. Если необходимо использовать несколько портов или IP адресов, то разделителем является символ «;».Стоит учитывать что если используется несколько портов то при использовании приложения операционная система может запросить повышенные привилегии.



Ключи сигнатуры

Перед использованием необходимо настроить используемые ключи и хранилища сертификатов. Подробнее об этом можно узнать в документации на СКЗИ Сигнатура. Основные параметры:

Наименование	Описание
Номер	Порядковый номер, в котором инициализируется этот ключ/хранилище
GUID	Уникальный идентификатор учетной записи
По-умолчанию	Если guid в запросе не передан, то будет использоваться эта учетная запись
Имя профиля	Используются в именованных профилях, наиболее часто используется при простой инициализации с профилем — My
Флаг	− Flag_Init_Nocrlupdate = 1 - не выполнять автоматическое обновление COC при инициализации; − Flag_Init_Checkexpired = 2 - показывать диалог с истекающими по времени объектами; − Flag_Init_Noldap = 4 - не использовать сетевой справочник; − Flag_Init_NoSaveCache = 32 - не сбрасывать объекты из кэша в локальный справочник по завершении работы; − Flag_Init_Registry = 64 - использовать профили Справочника из реестра вместо конфигурационного файла; − Flag_Init_UseAiaCdp = 1024 - Разрешить доступ к точкам AIA и CDP для загрузки сертификатов промежуточных ЦС и COC при построении цепочек; − Flag_Init_SilentKeyload = 2048 - Не выдавать пользовательский интерфейс при загрузке закрытого ключа; − Flag_Init_VerifyContext = 2147483648 - контекст без доступа к закрытому ключу.
PSE	Путь к ПСП (персональному справочнику пользователя). Строка вида pse://signed/F:\base\local.pse
Хранилище	Путь к ЛСП (локальному справочнику пользователя) file://F:\base\local.gdbm
Низкоуровневый интерфейс	Необходимо использовать данный интерфейс если предполагается работать с функциями чистой подписью. На текущей версии (1.4.1) такие контексты нельзя использовать для выполнение других операций

После настройки можно попробовать провести тестирование СКЗИ. При этом на каждом из ключей будет проведена операция подписания. Перед тестированием параметры ключей сигнатуры будут сохранены в локальный файл конфигурации, но не будут сохранены в конфигурации сервиса.

Логирование

В этой вкладке собраны все настройки связанные с логированием запросов.

- Писать файлы отладки. При активизации сохраняет в каталог отладки файлы с запросами и ответами к серверу. Дополнительно можно указать логировать ли все операции или только операции с критическими ошибками.

-Логирование времени операции. При этом режиме в каталог отладки сохраняется файл speedlog.txt. Где каждая строка это результат обработки одного запроса с временем в мс на каждый этап операции.

- Логировать критические ошибки. При этом режиме в каталог отладки сохраняется файл criticalLog.txt с текстом последней критической ошибки. Если работа возобновляется в нормальном режиме, файл удаляется.

- Логирование в бд. Возможно сохранить в Oracle следующие данные о запросах:

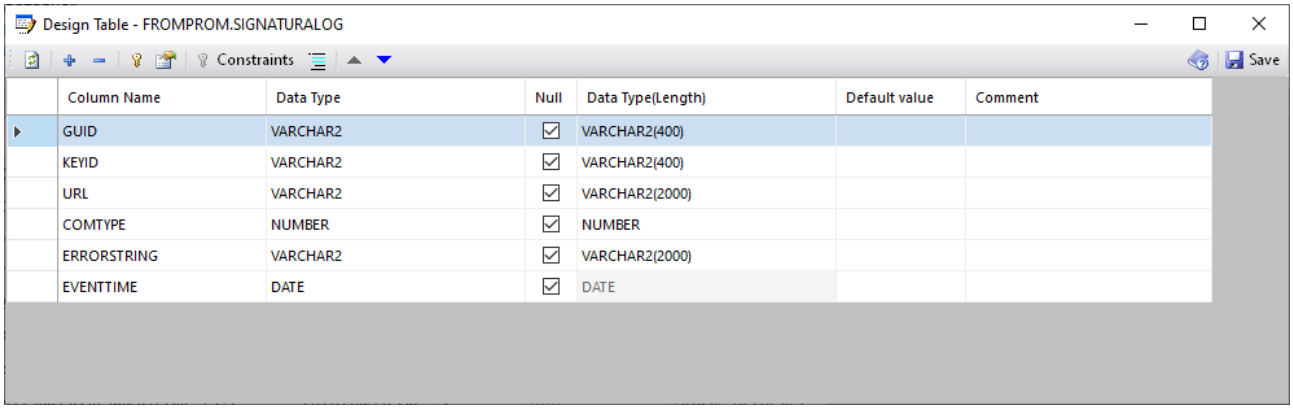
- GUID запроса
- Идентификатор ключа
- URL, откуда пришел запрос
- Тип операции

Номер	Тип операции
1	Получение информации о ключах
2	Инициализация с минимальными параметрами
3	Инициализация
4	Расширенная инициализация
5	Деинициализация
6	Получение хэша от файла
7	Получение хэша от блока памяти
8	Подписание файла
9	Подписание блока памяти
10	Проверка файла
11	Проверка блока памяти
12	Получение случайного числа
13	Шифрование блока памяти
14	Шифрование файла
15	Расшифрование блока памяти
16	Расшифрование файла
17	Подписание и шифрование блока памяти
18	Расшифрование и проверка блока памяти

19	Подписание и шифрование файла
20	Расшифрование и проверка файла
21	Получение статуса сервера
22	Проверка имперсанолизации
24	Подписание хэша (чистая подпись)
25	Проверка чистой подписи

- Строка с ошибкой
- Время события

Перед использованием необходимо завести пользователя базы данных с правами необходимыми для создания таблиц и создания в ней записей. В процессе работы Транссигнатура создаст таблицу Signaturalog



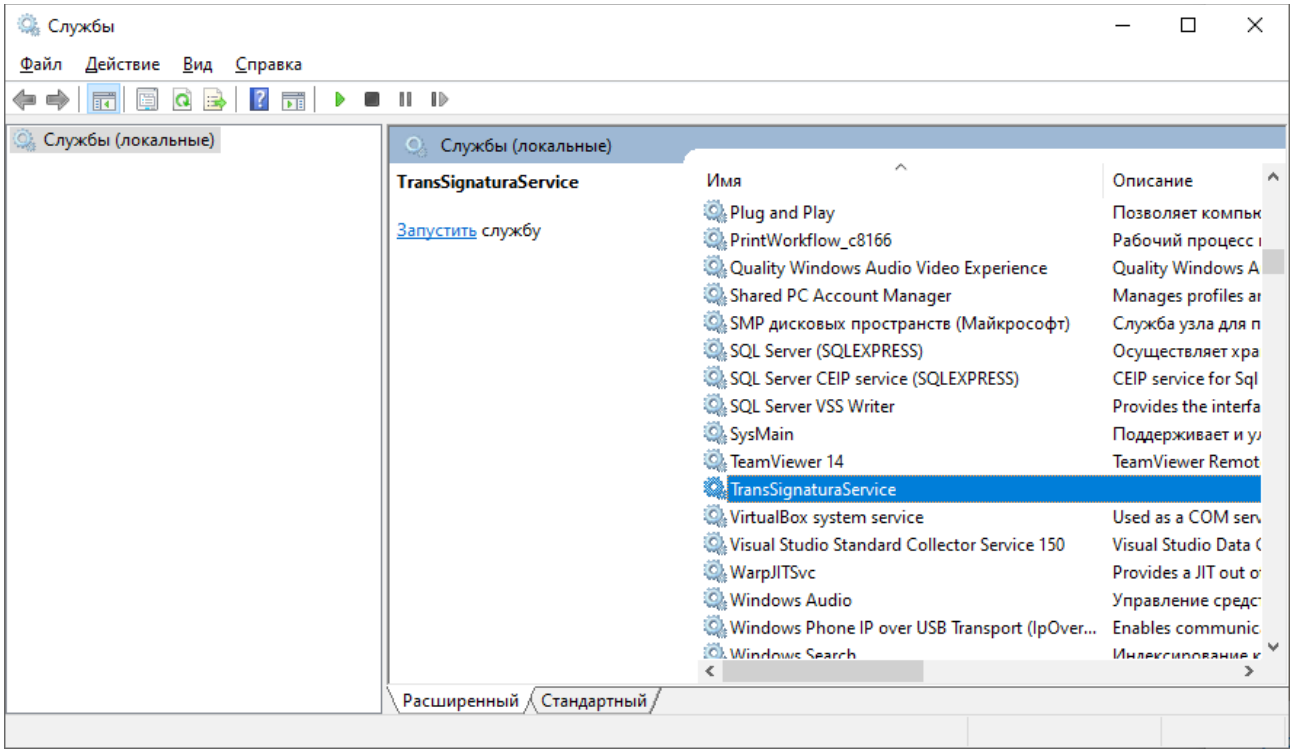
Строку подключения к БД необходимо сохранить в параметрах транссигнатуры. Формат строки соединения с бд зависит от используемой версии Oracle Client.

- Логирование времени операций в бд. В этом режиме в бд в таблицу signaturatimelog сохранятся информация о

- Времени операции
- GUID запроса
- Времени выполнения элементов операций в милисекундах

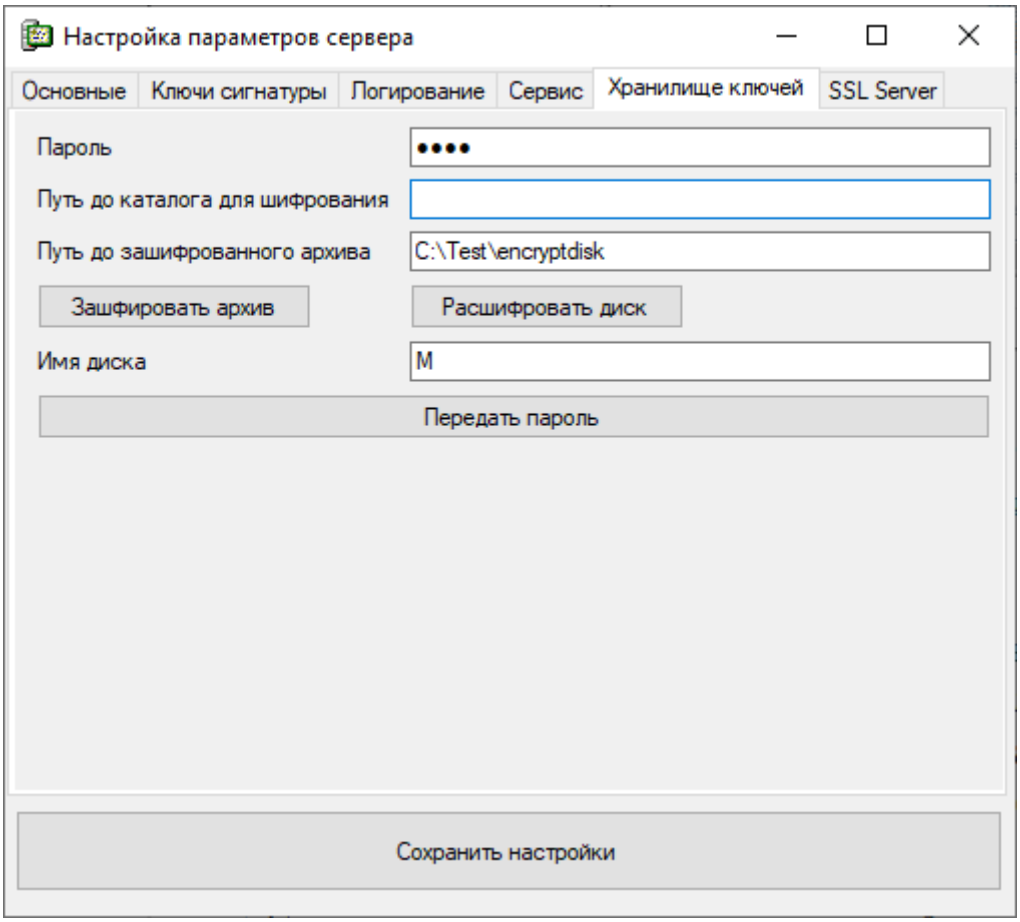
Сервис

Транссиг сервер может работать в режиме сервиса. Для установки и удаления сервиса необходимо запустить приложение для настройки параметров сервиса в режиме администратора. Если необходимо установить сервер, что бы он запускался от лица определенного пользователя, можно после установки воспользоваться стандартными настройками операционной системы (Панель управления → Администрирование → Сервисы). Наименование сервиса TransSignaturaService. Основной файл TransSignaturaService.exe. Каталог сервиса указывается при установке.



Хранилище ключей

Внимание! Данная функция является экспериментальной ее интерфейс и функционал не утвержден и не согласован. Возможны несоответствия с документацией.



Для защищенного хранилища можно использовать виртуальные диски. При этом ключи сигнатуры сохраняются в файл, защищенным паролем. При запуске администратор вводит этот пароль, транссигнатура сервер создает виртуальный диск, инициализирует сервер и отключает его. Эксперименты показали что работоспособность СКЗИ Сигнатуры при этом сохраняются. Порядок работы следующий

- Создается каталог с хранилищем ключей и сертификатов
- Указывается путь где будет храниться зашифрованных архив
- После нажатия кнопки Зашифровать архив получим файл с зашифрованными ключами. Файлы из каталога можно удалить.
- Можно проверить уже существующий архив с использованием сервиса Расшифровать диск.
- После этого необходимо указать имя диска, это имя не должно занята уже существующим.
- Пути к ключам сигнатуры необходимо изменить на новый диск.
- Для инициализации работы необходимо запустить настройки параметров сервера, ввести пароль и нажимаем передать пароль. При это происходит следующее

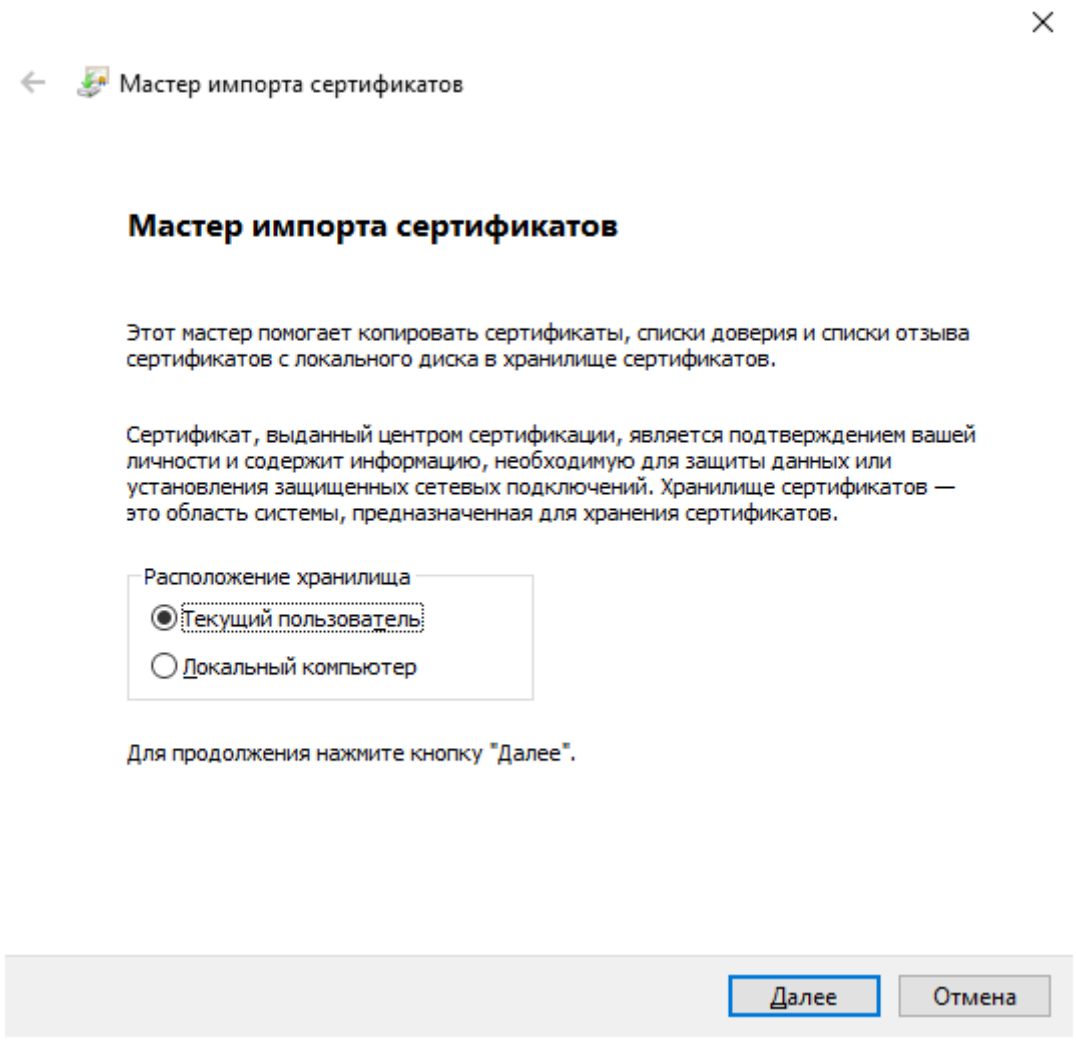
- Создается ramdisk с параметрами imdisk -a -s 100M m (имя монтирования) -o rem -p "/fs:fat /q /y"
- На него расшифруются данные
- Для каждого из ключей сигнатуры проводиться операция подсчета хэша, подписи и проверки
- Диск отключается imdisk -D -m (имя монтирования)

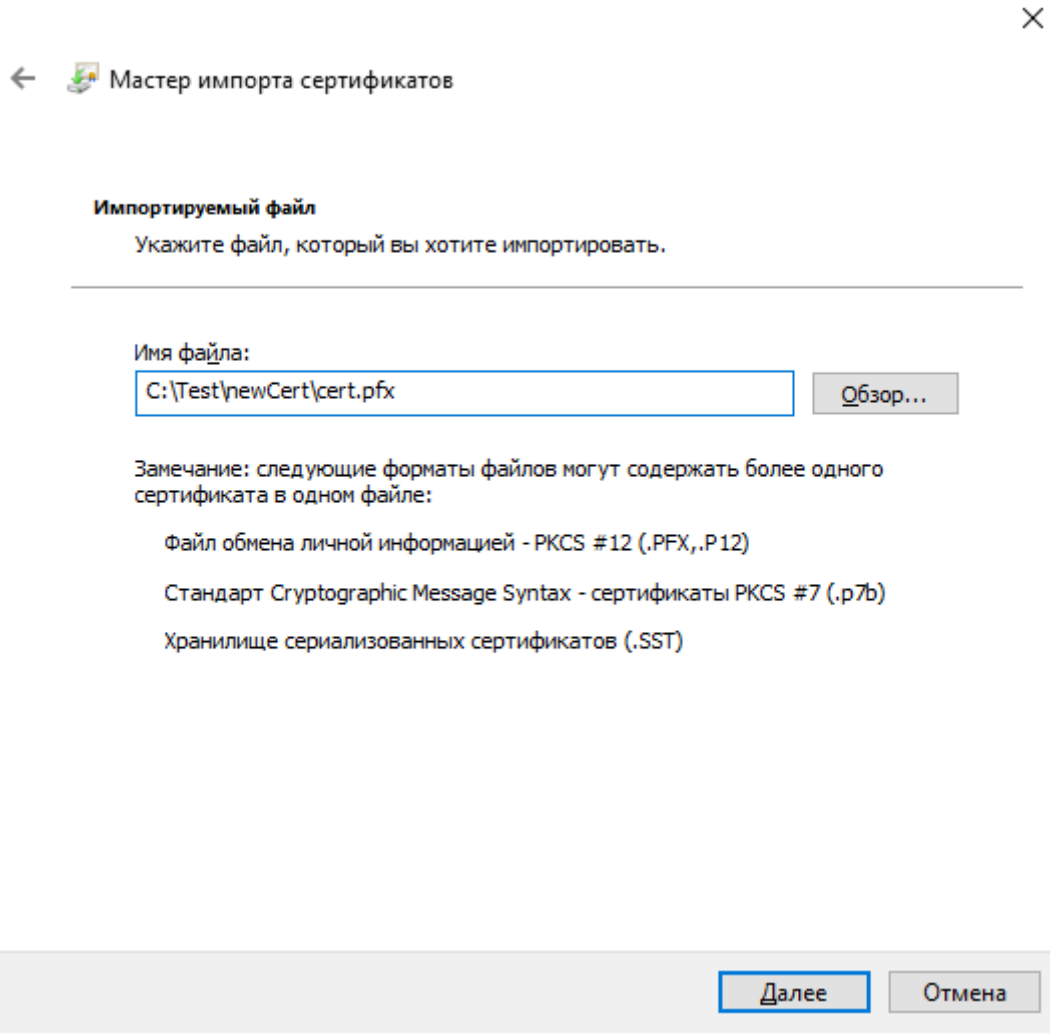
SSL Server

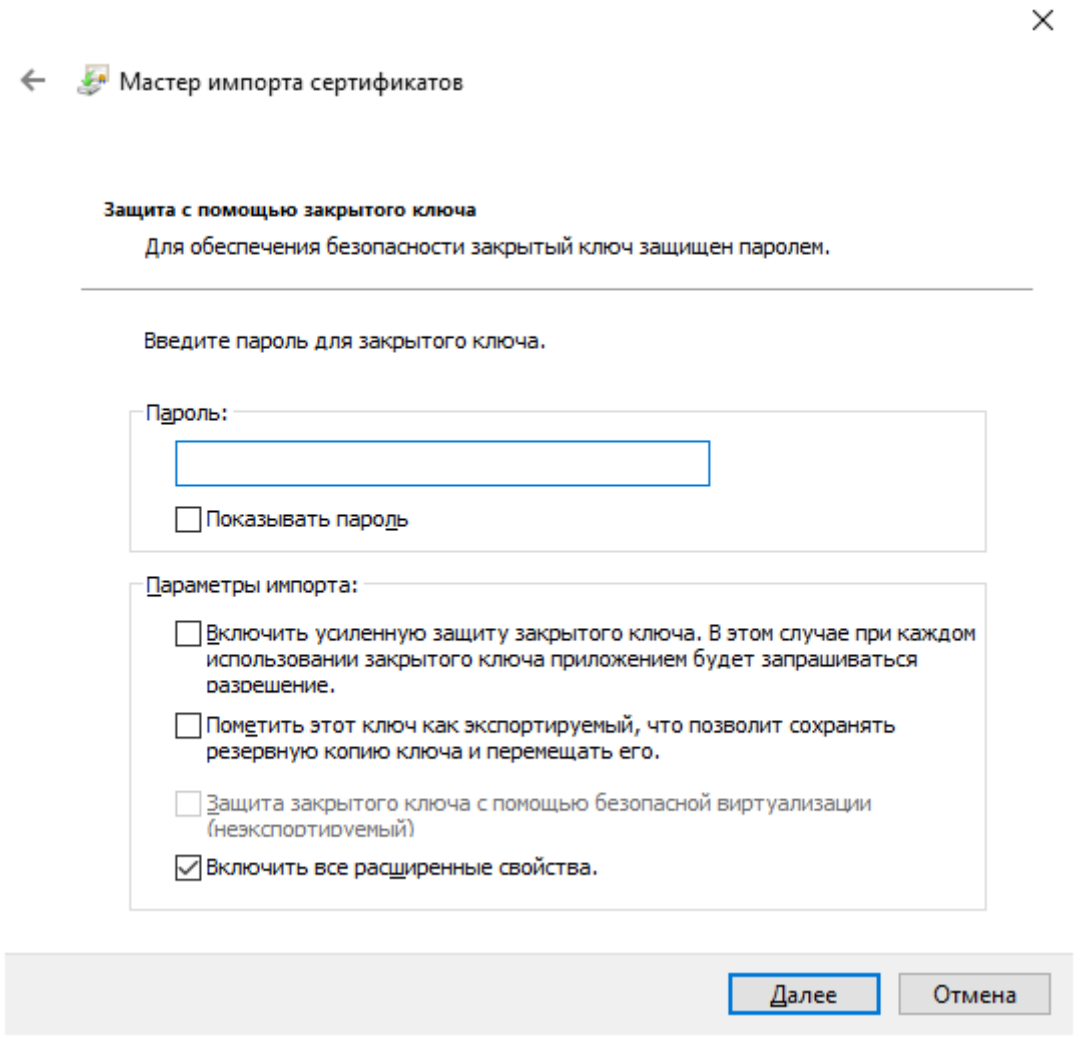
Внимание! Данная функция является экспериментальной ее интерфейс и функционал не утвержден и не согласован. Возможны несоответствия с документацией.

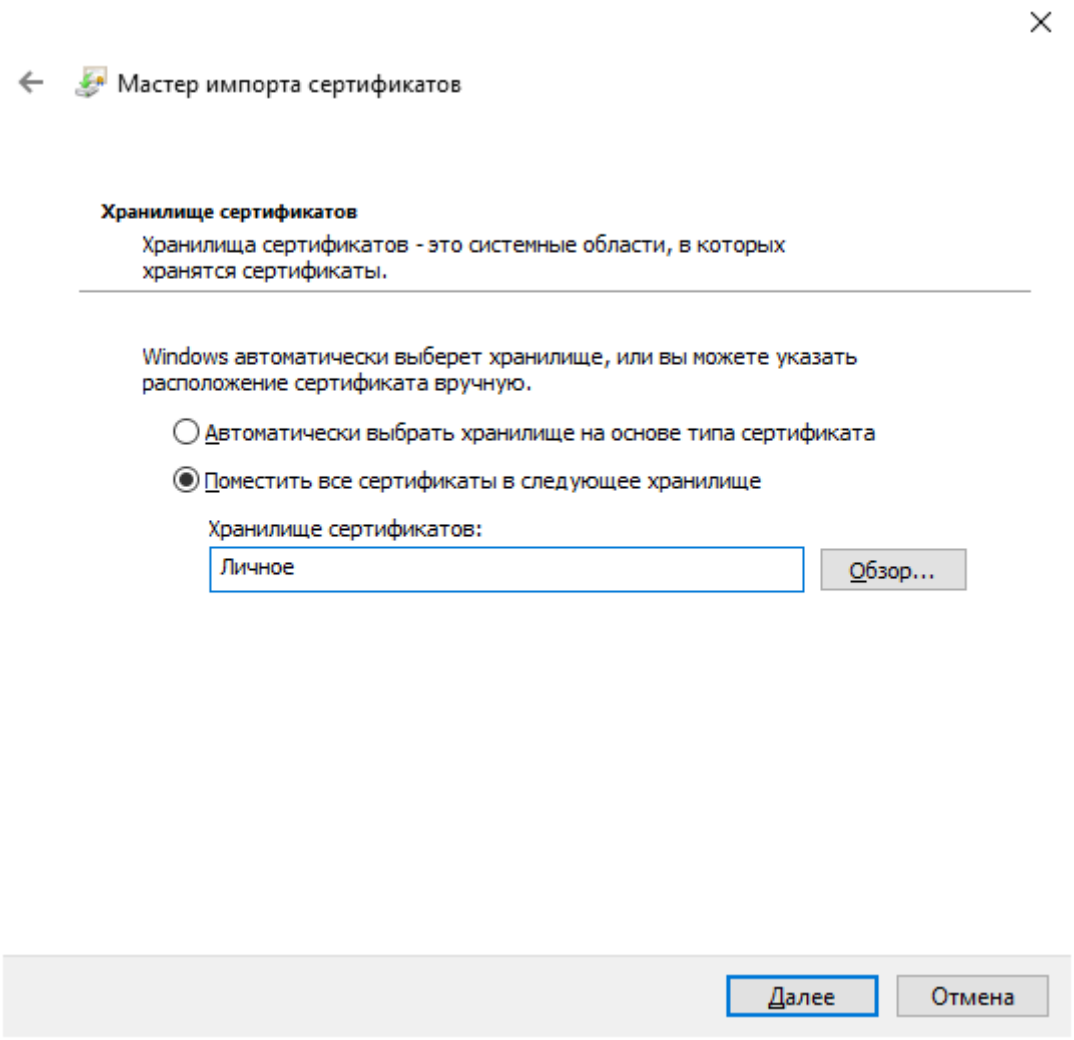
Для защиты передаваемых данных можно настроить работу SSL сервера. Порядок действий следующий.

- В УЦ Создается RSA SSL сертификат сервера и ключ и экспортируется для передачи в файл (.pfx).
- Этот ключ и сертификат устанавливается в локальное хранилище на сервер с помощью мастера импорта сертификатов




Мастер импорта сертификатов
Импортируемый файл
Укажите файл, который вы хотите импортировать.
Имя файла:
C:\Test\newCert\cert.pfx
Обзор...
Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:
Файл обмена личной информацией - PKCS #12 (.PFX,.P12)
Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)
Хранилище сериализованных сертификатов (.SST)
Далее
Отмена


Мастер импорта сертификатов
Защита с помощью закрытого ключа
Для обеспечения безопасности закрытый ключ защищен паролем.
Введите пароль для закрытого ключа.
Пароль:
Показывать пароль
Параметры импорта:
Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.
Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.
Защита закрытого ключа с помощью безопасной виртуализации (неэкспортируемый)
Включить все расширенные свойства.
Далее
Отмена



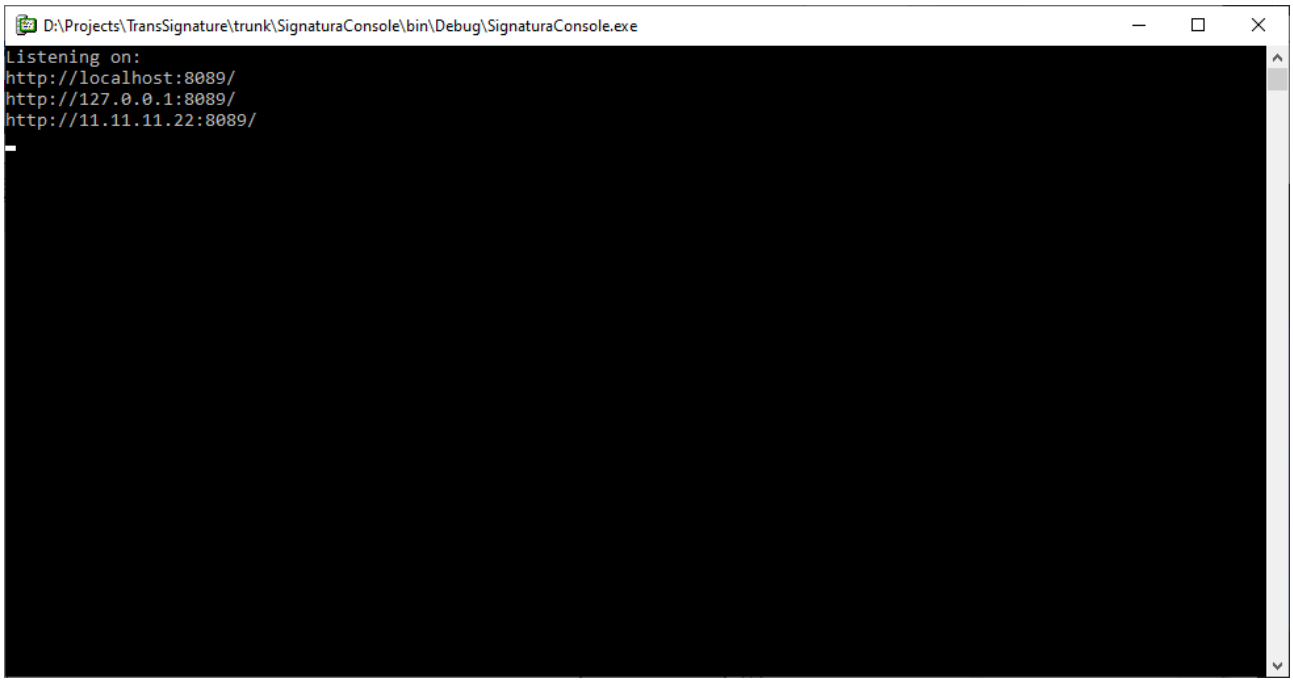
- После этого необходимо прописать этот ключ для использования в качестве SSL. Это делается либо через панель управления либо выполнением следующих команд от лица администратора
  - netsh http delete sslcert ipport=0.0.0.0:{SSLPort}",
  - netsh http add sslcert ipport=0.0.0.0:{SSLPort} certhash={certThumbprint} appid=\"{SSLAppID}\""

    Где SSLPort это будущий пот для SSL, certThumbprint берется из сертификата SSLAppID это случайный GUID.
- После этого можно настроить транссигнатуру сервер. Указав там параметры
  - Использовать SSL
  - Порт для SSL
  - Subject
  - Root Subject
  - Вид хранилища
- Проверку работы можно производить с использованием консольного приложения

Дополнительно можно ограничить обращения пользователей включив двухсторонний SSL (галочка требовать сертификат клиента) или указав список разрешенных адресов (разделитель ; или , или перенос строки).

Консольное приложение

Для тестирования работы без установки сервиса можно воспользоваться консольным приложением. По функционалу оно аналогично, но позволяет в реальном времени видеть ошибки инициализации приложения.



Общий процесс установки и настройки приложения

Перед установкой сервера транс-сиг необходимо настроить все части СКЗИ Сигнатуры. Подробнее об этом в документации к:

- СКЗИ СКАД Сигнатура
- СЗИ СКАД: Справочник сертификатов
- СКАД Сигнатура SDK
- Oracle Client

Следующим шагом является получение ключей и справочников сертификатов. Это файлы

- local.gdbm
- local.pse
- файл с ключом *.vdk

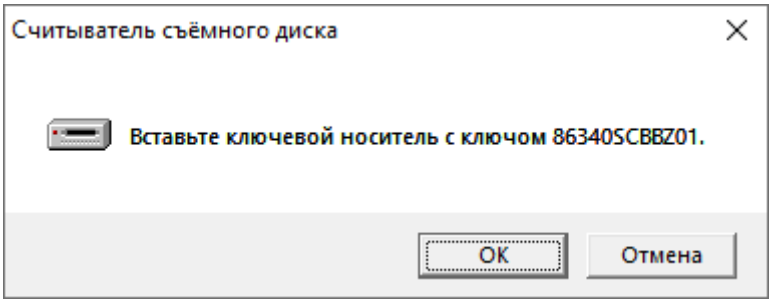
Эти файлы необходимо поместить на внешний извлекаемый носитель (флешку). При этом рекомендуется следующая структура каталогов.

- Base1 (каталог для первого справочника)
  - local.gdbm
  - local.pse
- Base2 (каталог для второго справочника)
  - local.gdbm
  - local.pse
- BaseN ……
- vdkeys (каталог с ключами)
  - 12***01.vdk
  - 8****01.vdk
  - ….

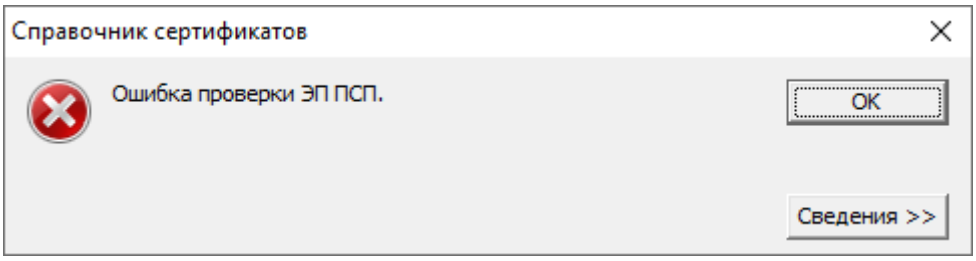
Если таковой носитель отсутствует или его использование не возможно, то можно воспользоваться специальными приложениями для эмуляции носителя (например ImDisk).

После этого необходимо открыть справочник сертификатов и пройти первичную установку справочника. Если используется несколько ключей (хранилищ) то нет необходимости проводить отдельную остановку второго и последующего ключа. Если данная операция уже производилось и происходит смена ключей, то порядок работ в этом случае выглядит следующим.

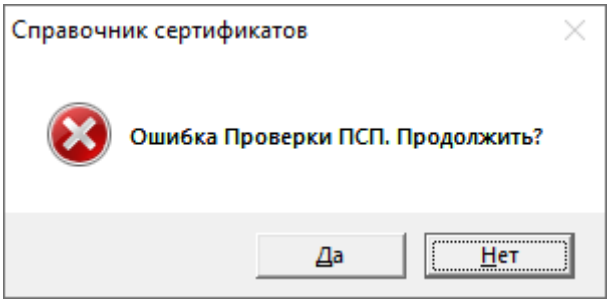
На предложение вставить ключевой носитель. Жмем Отмена.



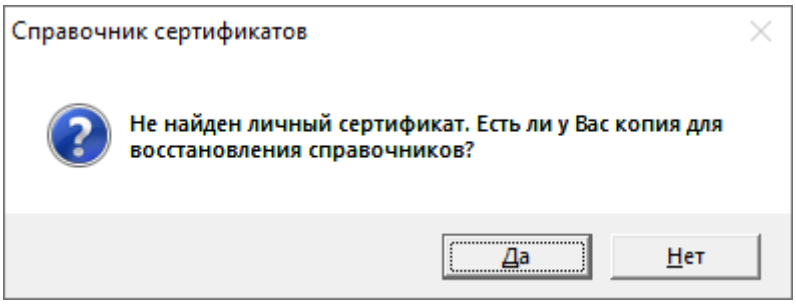
Ошибка проверки ЭП ПСП. Жмем Ок.



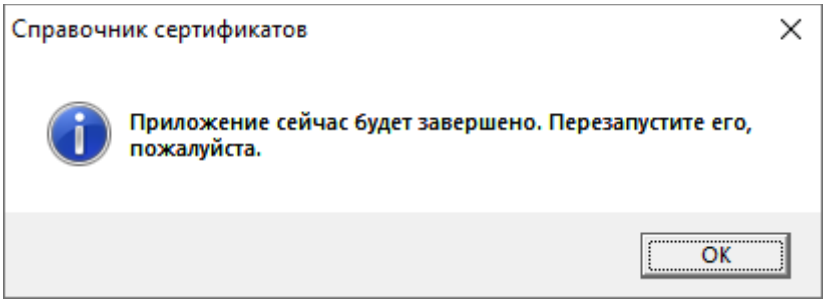
Ошибка проверки ПСП. Жмем Да.



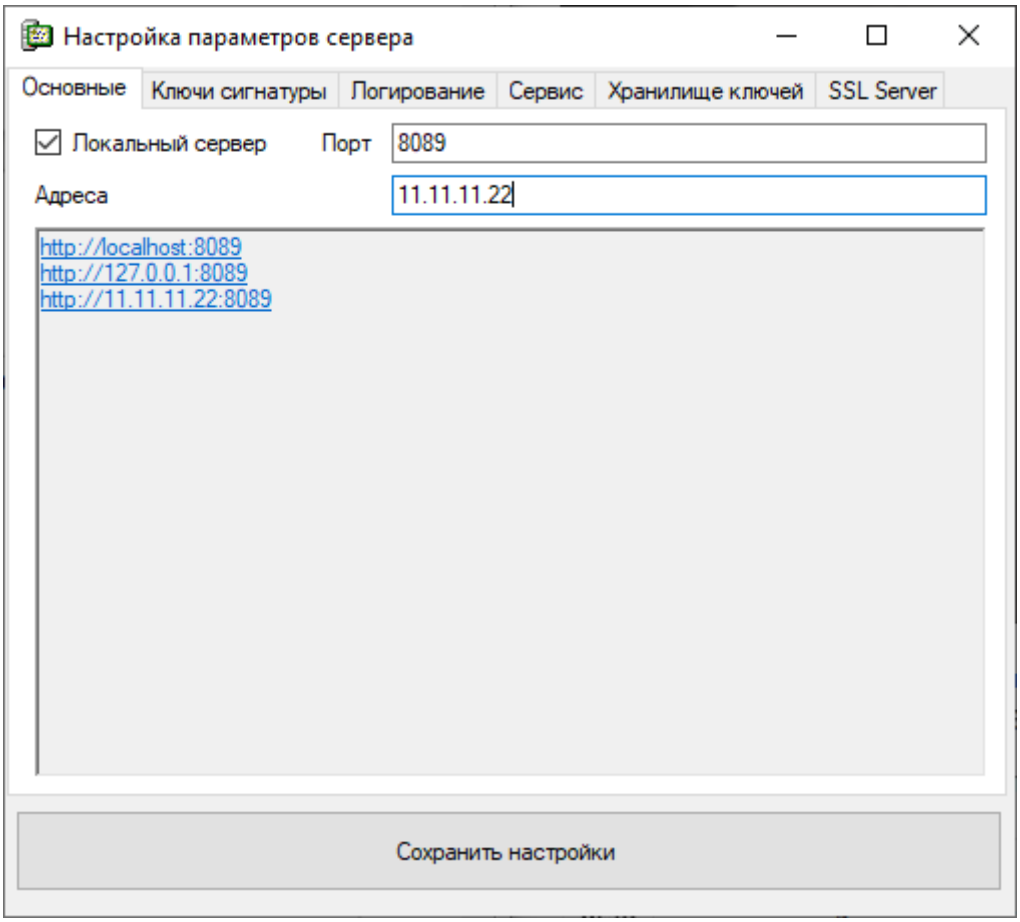
На предложение восстановления. Жмем Да.



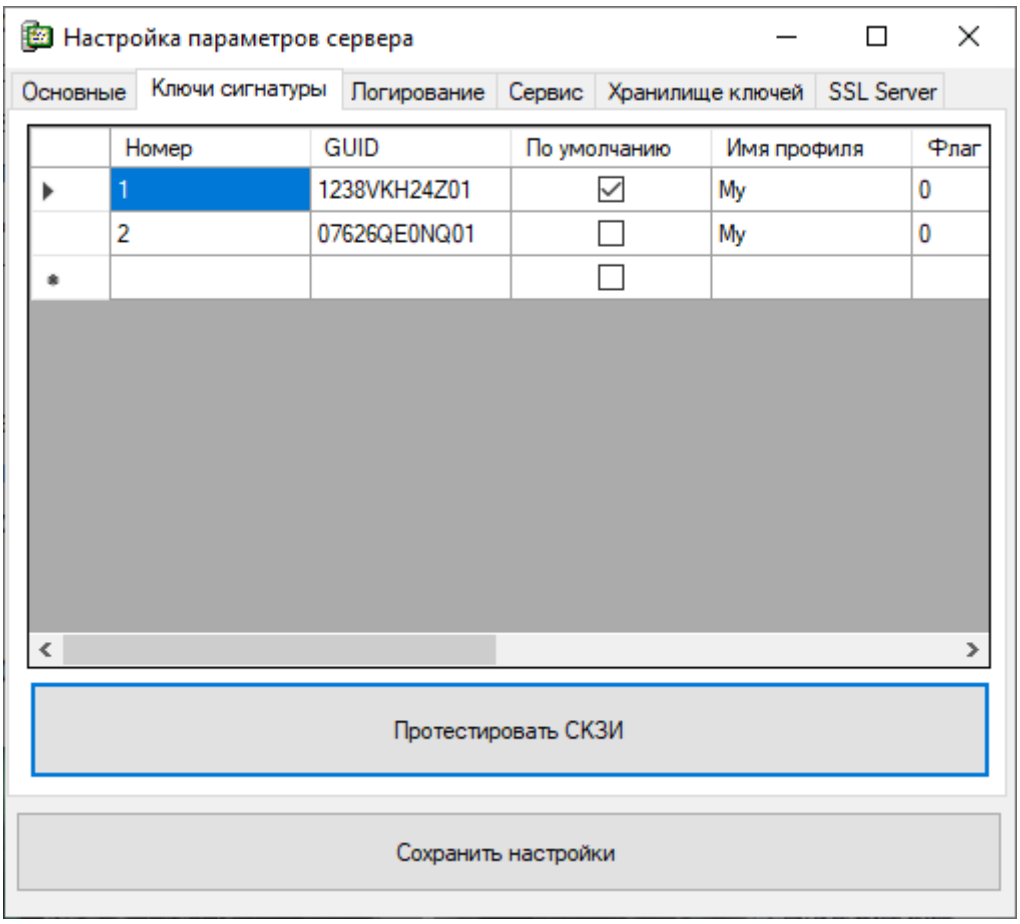
Указываем каталог base, со справочниками сертификатов и перезапускаем приложение.



Производим установку транссиг сервера. И открываем его для первичной настройки. После изменения какого либо параметра необходимо нажимать Сохранить настройки.



В данном окне необходимо оставить один внешний адрес, через который будут идти обращения к серверу. Галочку локальный сервер рекомендуется оставлять для целей отладки и тестирования.

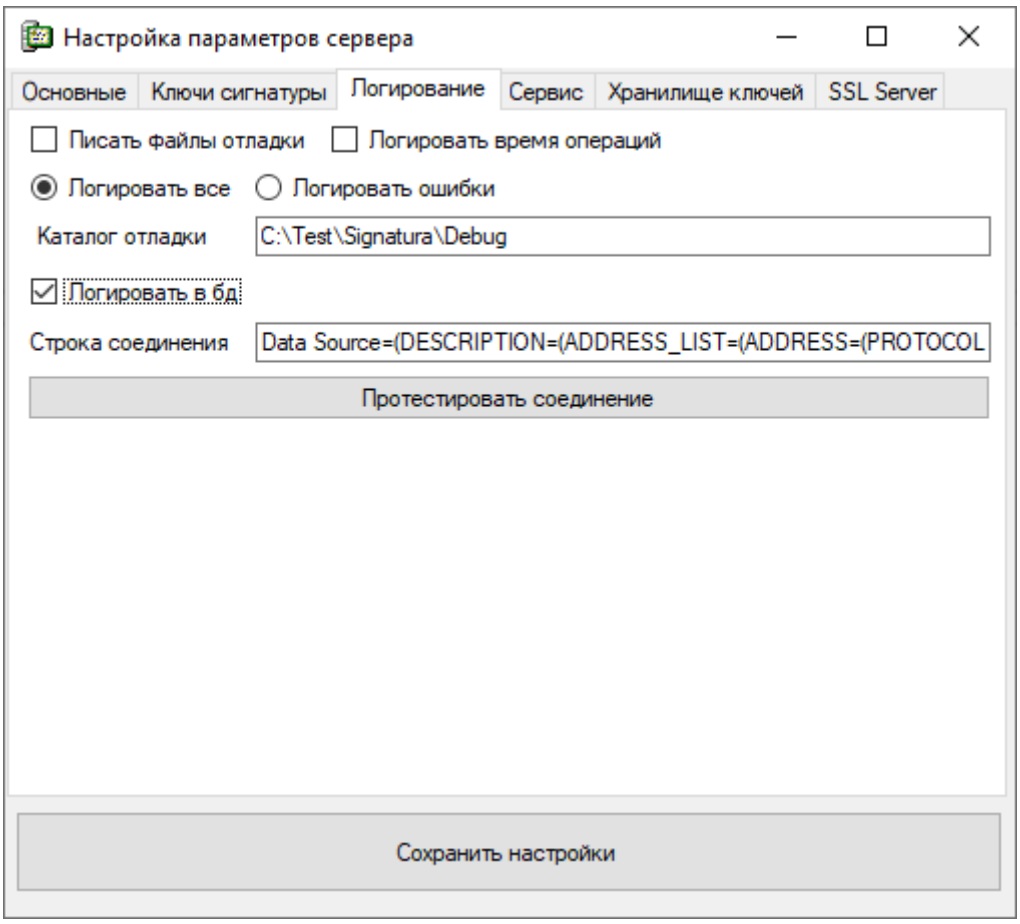


Необходимо установить параметры ключей сигнатуры где важно следующее.

- GUID – строка, если не требуется чего-то особенного, равная идентификатору ключа (имени файла *.vdk)
- Один из ключей рекомендуется поставить по умолчанию
- Имя профиля — My
- PSE вида pse://signed/F:\base\local.pse
- LocalStorage вида file://F:\base\local.gdbm
- Флаги — 0

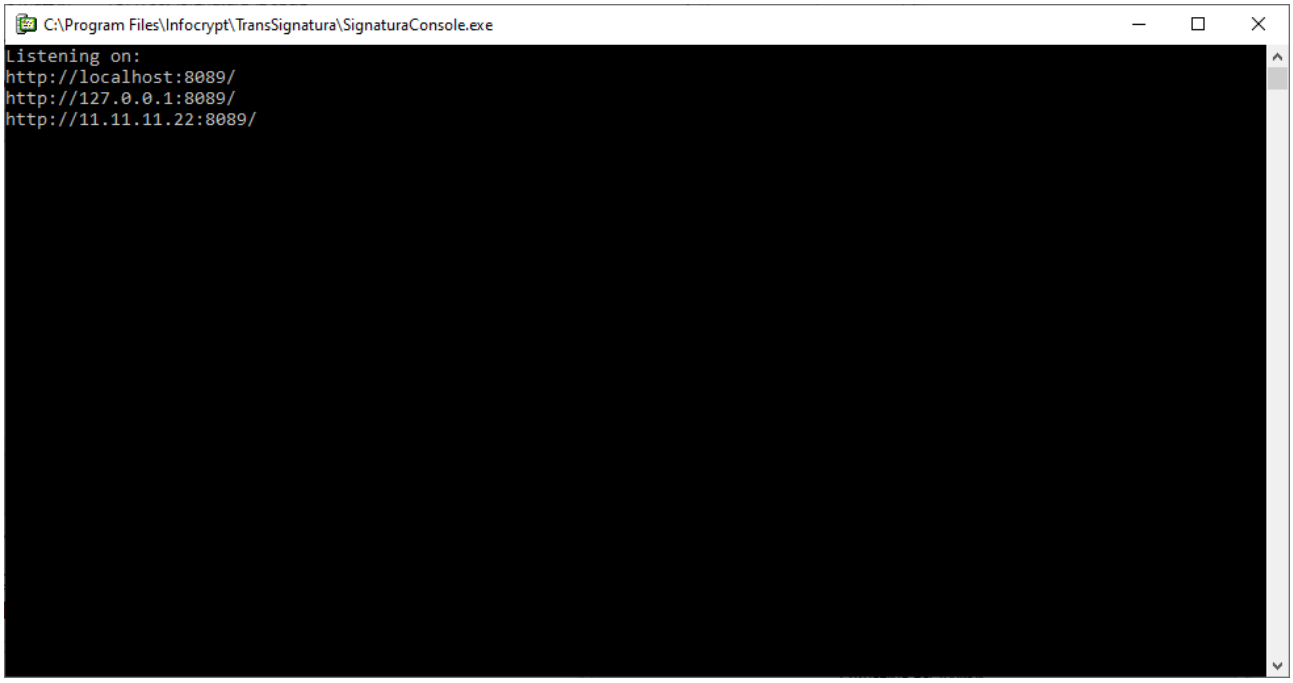
После установки необходимо воспользоваться сервисом тестирования СКЗИ. Если происходит ошибка то необходимо:

- Проверить правильность написание путей.
- Попробовать остановить текущие запущены части транссиг сервера, а именно приложение для настройки, консоль и сервис. После этого запустить только настройки и повторить тестирование.
- Запустить справочник сертификатов СКЗИ Сигнатруа и попробовать использовать этот справочник как основной. После этого проанализировать сообщение СКЗИ. Возможно истек срок действия ключей и сертификатов



На вкладке логирование необходимо установить параметр логировать в бд и указать строку соединения с бд. Для проверки можно воспользоваться сервисом протестировать соединения. Саму строку можно получить у администраторов Oracle.

После этого рекомендуется сохранить настройки, запустить локальную консоль сервера транссигнатуры и проверить работоспособность с помщью тестовой Транссиг клиента или другого приложения.



После успешного проведенного тестирования необходимо установить сервис, для этого откройте настройку параметров сервиса в режиме администратора, если сервис будет запускаться не от лица системы, а от лица конкретного пользователя то необходимо указать его логин и пароль (это так же можно сделать позже через панель управления).