

Axiom Lab

Axiom Lab представляет собой неполные программные модели аппаратных ключей Рутокен ЭЦП 3.0 и JaCarta-2 PKI/ГОСТ, исполненные в виде динамических библиотек, обеспечивающих доступ к моделям через интерфейс PKCS#11. Кроме того, в состав Axiom Lab входит утилита для их конфигурирования. Функционал моделей достаточен для их использования совместно с УТМ ЕГАИС.

Возможности Axiom Lab:

- Имитация аппаратных ключей Рутокен ЭЦП 3.0 и JaCarta-2 PKI/ГОСТ на уровне, достаточном для функционирования УТМ
- Использование сертификатов ГОСТ и RSA, хранящихся (вместе с соответствующими им закрытыми ключами)
 1. В системных хранилищах сертификатов (в контексте компьютера)
 2. На аппаратных ключах Рутокен, JaCarta, ESmart и MS Key K (Ангара+)
 3. В файлах JKS, PEM, PKCS12 (PFX)
- Формирование сертификатов RSA через утилиту конфигурирования (в том числе с использованием МЧД)
- Репликация УТМ, быстрое переключение реплик с одной версии УТМ на другую без потери данных

Требования:

- Операционная система Microsoft Windows (7 и выше)
- Для работы с сертификатами, хранящимися в системных хранилищах – криптопровайдеры, использованные для формирования ключевых контейнеров и закрытых ключей
- Для работы с сертификатами, хранящимися на аппаратных ключах – оригинальные библиотеки PKCS#11 от производителей этих ключей
- Для работы с сертификатами, хранящимися в файлах – наличие OpenSSL с движком ГОСТ
- Для загрузки торговых точек из ЕГАИС – наличие OpenSSL
- Для функционирования УТМ – установленный экземпляр УТМ и действующий сертификат ГОСТ (КЭП) с соответствующим ему закрытым ключом

Установка и удаление

Axiom Lab поставляется в виде программы-установщика (инсталлятора), одновременно являющейся средством обновления установленного программного продукта.

По умолчанию Axiom Lab устанавливается в директорию

- "C:\Program Files (x86)\Axiom Software\Axiom Lab" для 64-х битных систем
- "C:\Program Files\Axiom Software\Axiom Lab" для 32-х битных систем

В директорию установки Axiom Lab устанавливаются утилита конфигурирования и данное руководство пользователя.

Для хранения персистентных данных Axiom Lab использует директорию "C:\ProgramData\Axiom Lab" (директорию данных). В нее устанавливаются база данных в формате SQLite и файлы динамических библиотек, обеспечивающих доступ к моделям аппаратных ключей через интерфейс PKCS#11. Тут же хранится файл "Settings.json" с конфигурацией Axiom Lab.

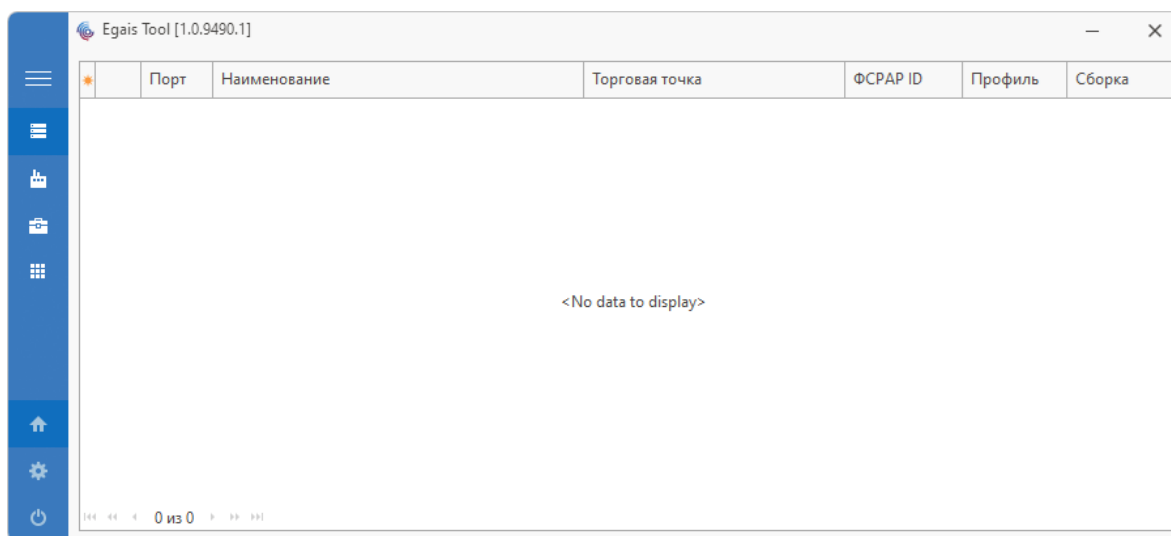
Перед установкой или обновлением Axiom Lab рекомендуется остановить все реплики УТМ, закрыть все экземпляры утилиты конфигурирования и открытого из директории установки руководства пользователя.

При обновлении Axiom Lab обновляются утилита конфигурирования, руководство пользователя и файлы динамических библиотек. База данных и файл конфигурации не обновляются.

При деинсталляции Axiom Lab удаляются утилита конфигурирования, руководство пользователя и файлы динамических библиотек. База данных и файл конфигурации сохраняются и могут быть использованы в будущем.

Утилита конфигурирования

Утилита конфигурирования (EgaisTool) предназначена для настройки Axiom Lab в части обеспечения функционирования УТМ:



Панель навигации позволяет переключаться между разделами утилиты конфигурирования. Разделы разбиты на группы (пиктограммы в нижней части панели навигации):

- Главное меню
- Настройки приложения

Группа "Настройки приложения" включает в себя следующие разделы:

- Основные настройки приложения
- Настройки хранилищ сертификатов
- Настройки лицензирования

Группа "Главное меню" включает в себя следующие разделы:

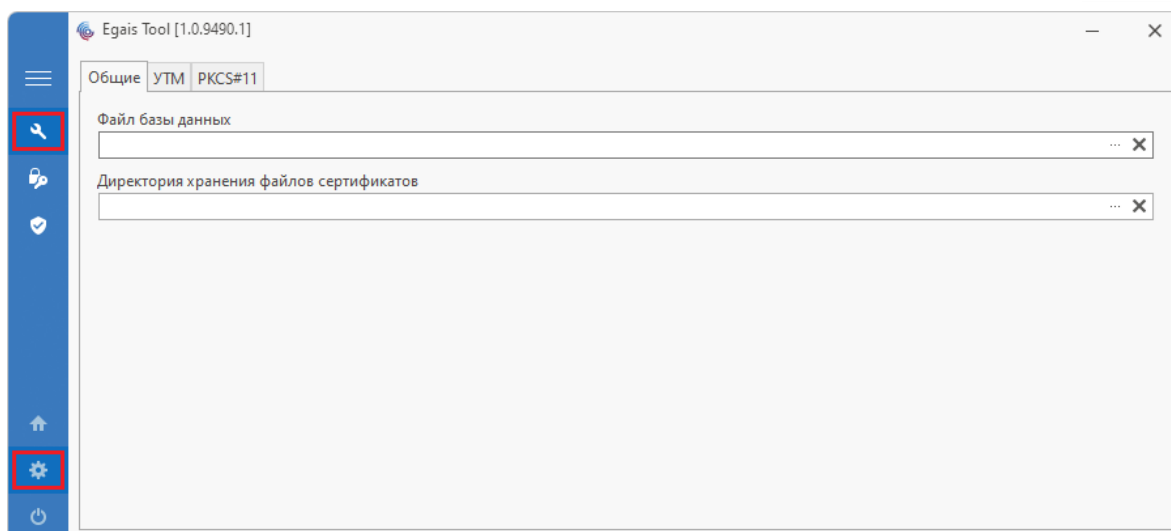
- Управление УТМ (данный раздел отображается при запуске утилиты конфигурирования)
- Справочник организаций
- Реестр МЧД
- Версии УТМ

Для того чтобы утилита конфигурирования имела доступ к закрытым ключам сертификатов, хранящихся в системных хранилищах контекста компьютера, ее следует запускать с правами администратора.

Основные настройки приложения

Раздел "Основные настройки приложения" представляет собой группу вкладок, на каждой из которых можно (но не обязательно нужно) определить тот или иной параметр функционирования как утилиты конфигурирования, так и Axiom Lab. Отсутствие значения для того или иного параметра означает, что используется значение по умолчанию (как правило, его более чем достаточно).

Вкладка "Общие"

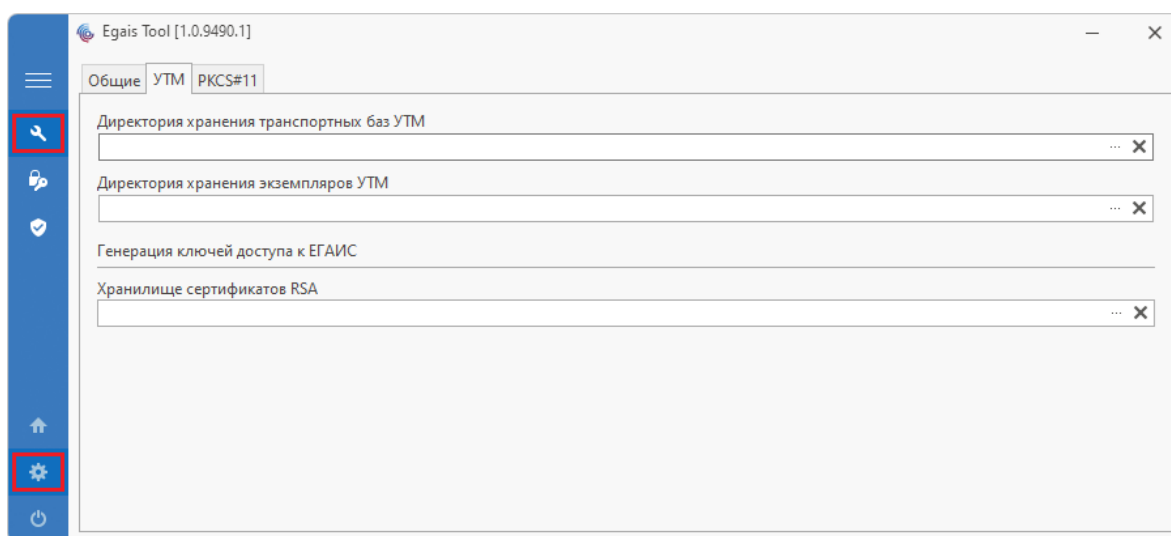


Вкладка "Общие" позволяет определить

- Файл базы данных (по умолчанию используется тот, что лежит в директории данных Axiom Lab)
- Директорию хранения файлов сертификатов (по умолчанию используется поддиректория "CertStorage" директории данных Axiom Lab)

Директория хранения файлов сертификатов используется как первичная локация при выборе файлов сертификатов.

Вкладка "УТМ"



Вкладка "УТМ" позволяет определить

- Директорию хранения транспортных баз УТМ
- Директорию хранения экземпляров УТМ
- Хранилище сертификатов, используемое при генерации ключей доступа к ЕГАИС (сертификатов RSA) через соответствующий раздел домашней страницы УТМ

Утилита конфигурирования позволяет реплицировать УТМ, позволяя одновременно функционировать нескольким торговым точкам. Для функционирования каждой торговой точки требуется собственная транспортная база УТМ (обычно это поддиректория "transportDB" директории транспортного сервиса УТМ).

Утилита конфигурирования дает возможность создания множества торговых точек, при этом их может быть настолько много, что одновременное функционирование каждой из них на отдельной реплике УТМ становится невозможной в силу отсутствия соответствующих аппаратных ресурсов (CPU, RAM).

Утилита конфигурирования позволяет переключать реплики УТМ с одной торговой точки на другую, давая возможность по очереди использовать все торговые точки на всех имеющихся репликах УТМ.

Обычно при переключении УТМ транспортные базы торговых точек удаляются и пересоздаются, при этом хранящиеся в них документы (как входящие, так и исходящие) теряются.

Для того чтобы обеспечить сохранность транспортных баз торговых точек, каждой из них необходимо прописать директорию хранения транспортной базы УТМ. Их централизованным хранилищем является директория хранения транспортных баз УТМ.

При отсутствии необходимости переключения торговых точек между репликами УТМ директории хранения транспортных баз УТМ торговых точек могут оставаться пустыми (что не дает гарантии сохранности транспортных баз УТМ, например, при удалении реплик УТМ).

При установке УТМ той или иной версии в системе создается его единственный экземпляр, состоящий из транспортного сервиса, расположенного в поддиректории "transporter" директории установки УТМ. При необходимости работы с УТМ иной версии требуется удалить ранее установленный, после чего установить новый. Вместе с тем требуется оставить в сохранности состояние транспортного сервиса УТМ (его конфигурацию, логи, файлы поддиректории "xml").

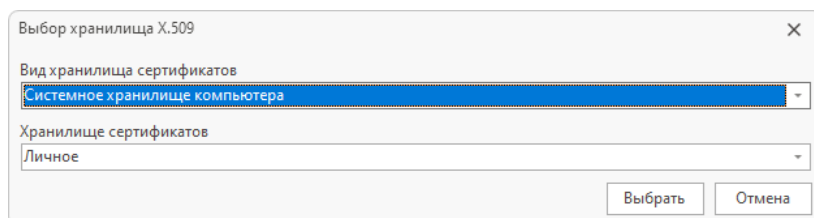
Состояние каждой реплики УТМ хранится в отдельной директории (имя которой соответствует номеру порта транспортного сервиса УТМ), эквивалентной директории "transporter". Директории реплик УТМ создаются и хранятся в директории хранения экземпляров УТМ.

Домашняя страница УТМ позволяет генерировать ключи доступа к ЕГАИС (сертификаты RSA торговых точек):

The screenshot shows the web interface of the Universal Transport Module (УТМ). The header includes the EGAIS logo and the text 'Универсальный Транспортный Модуль' and 'Федеральная служба по контролю за алкогольным и табачным рынками'. The main content area displays a progress bar with four steps: 1. Выбор роли..., 2. Выбор места осуществления деяте..., 3. Подтвердени..., 4. Резул... Below the progress bar, there is a section titled 'Выберите место осуществления деятельности или ТС' with two radio button options: 'Место осуществления деятельности' and 'Транспортное средство'. A 'Продолжить' button is located at the bottom of this section. On the left side, there is a sidebar menu with sections 'Документы' (containing 'Входящие' and 'Исходящие') and 'Сервисы' (containing 'Проверка продукции', 'Генерация ключа доступа к ЕГАИС', 'Добавление организации', 'Уведомление о начале оборота АП', 'Добавление ССП', and 'Выдача ФСМ').

Такие сертификаты формируются на аппаратных ключах, используемых для функционирования УТМ. При использовании Axiom Lab аппаратный ключ может отсутствовать, да и не всегда имеет смысл формировать сертификат RSA именно на него, ведь Axiom Lab позволяет использовать сертификаты, хранящиеся в системных хранилищах и в файлах.

Утилита конфигурирования позволяет указать точное расположение генерируемых через домашнюю страницу УТМ ключей доступа к ЕГАИС:



Генерация ключей доступа к ЕГАИС при неопределенном хранилище сертификатов RSA завершается ошибкой **"Не удалось записать RSA сертификат. Попробуйте еще раз"**.

Вкладка "PKCS#11"



Axiom Lab позволяет использовать сертификаты ГОСТ и RSA, хранящиеся (вместе с соответствующими им закрытыми ключами) на аппаратных ключах Рутокен, JaCarta, ESmart и MS Key K. Доступ к ключам осуществляется через оригинальные библиотеки от производителей аппаратных ключей посредством интерфейса PKCS#11.

Axiom Lab считает, что соответствующие библиотеки уже установлены в системе (располагаются в системных директориях) и пытается использовать именно их.

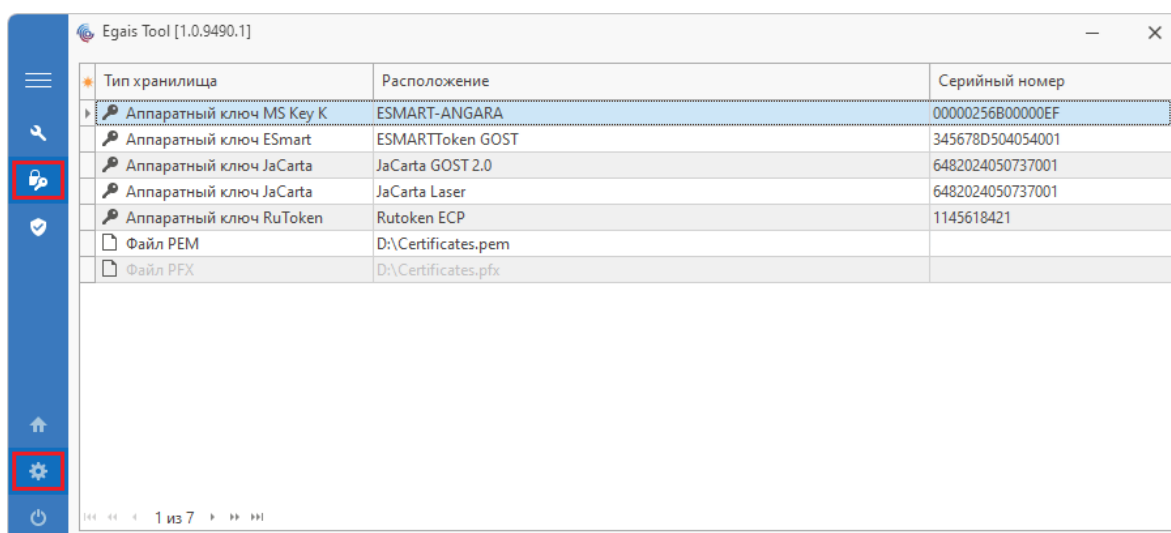
В том случае, когда имеется необходимость использовать какую-либо особенную библиотеку вместо той, что установлена (либо оригинальная библиотека не установлена, но необходимо использовать какую-то конкретную), достаточно указать полный путь к файлу этой библиотеки:



Необходимо помнить о том, что в дальнейшем данные библиотеки будут использоваться УТМ для доступа к соответствующим аппаратным ключам. Сам УТМ является 32-х битным, поэтому нужно выбирать именно 32-х битные библиотеки.

Настройки хранилищ сертификатов

Как правило, при использовании сертификатов, хранящихся на аппаратных ключах или в файлах, бывает необходимо указывать некий секрет (пин-код или пароль) для доступа к соответствующим закрытым ключам. Чтобы избежать многократный ввод секретов, можно использовать реализованный в Axiom Lab механизм хранилищ сертификатов:



Хранилище сертификатов является записью в конфигурации Axiom Lab, однозначно определяющей физическое хранилище (тип, расположение, уникальный идентификатор) и секрет для доступа к нему. Секрет хранится в зашифрованном виде, так что просто "подсмотреть" его не получится.

Утилита конфигурирования подсвечивает хранилища сертификатов в зависимости от их состояния:

- Серым подсвечиваются физически отсутствующие (удаленные) файловые хранилища сертификатов

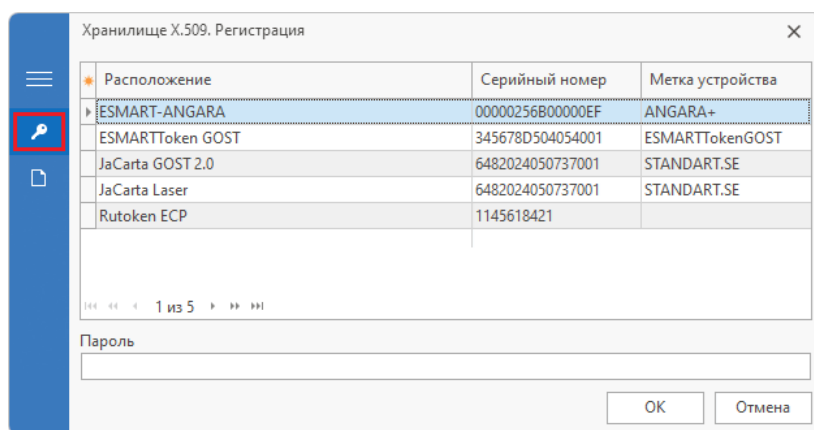
Все операции с хранилищами сертификатов осуществляются через контекстное меню списка хранилищ сертификатов утилиты конфигурирования.

Регистрация хранилищ сертификатов

Хранилища сертификатов регистрируются через специальный диалог, позволяющий зарегистрировать

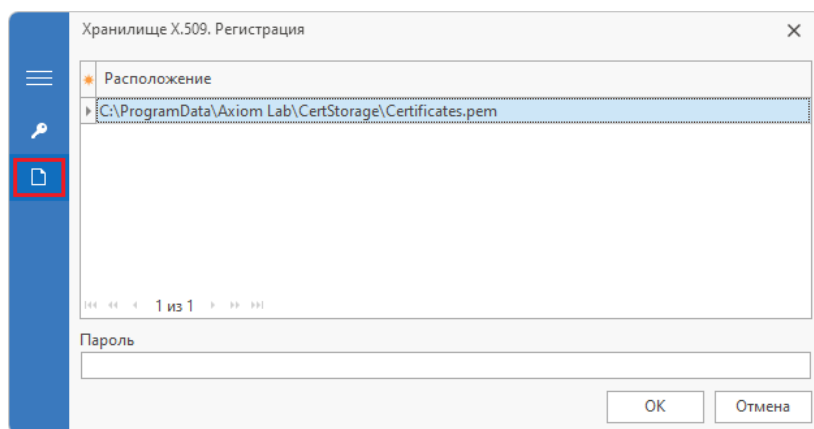
- Апплеты аппаратных ключей (аппаратные ключи вроде JaCarta бывают комбинированными и могут нести на своем борту несколько узкоспециализированных апплетов – каждый со своим пин-кодом)
- Файловые хранилища (JKS, PEM, PFX), для доступа к которым требуется знание пароля

Апплеты аппаратных ключей регистрируются в разделе "Аппаратный ключ" диалога. Для регистрации апплета аппаратного ключа достаточно выбрать нужный апплет нужного аппаратного ключа в списке и указать секрет для доступа к нему:



Список апплетов строится автоматически с использованием установленных в системе библиотек для работы с аппаратными ключами через интерфейс PKCS#11 с учетом [соответствующих настроек](#).

Файловые хранилища регистрируются в разделе "Файл" диалога – достаточно выбрать нужный файл в списке и указать секрет для доступа к нему:

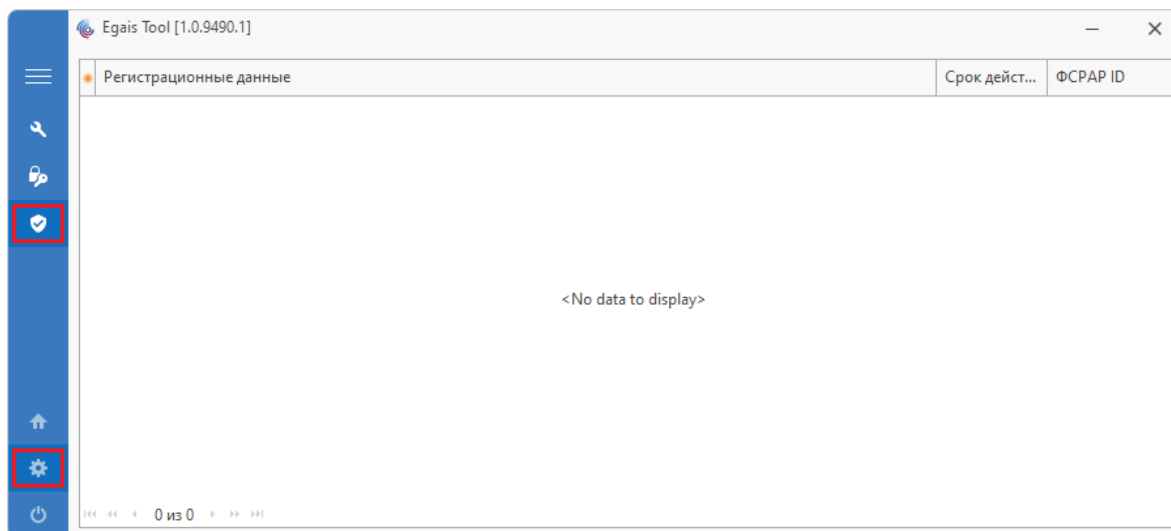


Список содержит найденные в директории хранения файлов сертификатов (с учетом [соответствующих настроек](#)) файлы поддерживаемых типов (JKS, PEM, PFX). Контекстное меню списка дает возможность дополнять его произвольными файлами поддерживаемых типов.

Для работы с файловыми хранилищами сертификатов требуется наличие OpenSSL с движком ГОСТ.

Настройки лицензирования

Для корректной работы Axiom Lab требуется регистрация – предоставление специальных данных, по которым будет сделан однозначный вывод о возможности или невозможности функционирования.



Регистрационные данные могут комбинировать в себе одно или несколько ограничений:

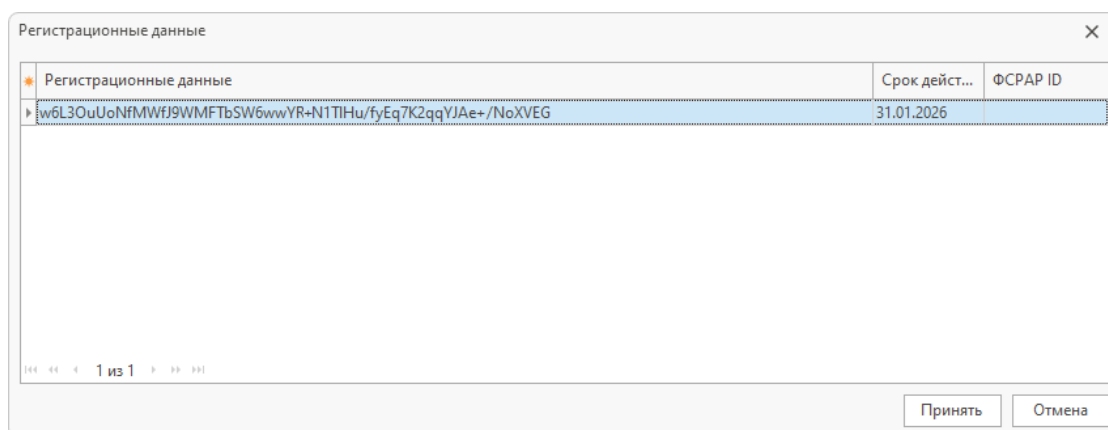
- Дата начала действия регистрационных данных (до этой даты регистрационные данные считаются недействительными)
- Дата окончания действия регистрационных данных (после этой даты регистрационные данные считаются недействительными)
- Идентификатор ФСРАР (FSRAR_ID) торговой точки сертификата RSA (регистрационные данные считаются действительными только при использовании действующего сертификата RSA с соответствующим значением поля CN)

Регистрационные данные ограничивают Axiom Lab исключительно в операциях подписания данных с использованием тех или иных сертификатов в той или иной момент времени. Любой иной функционал Axiom Lab не подпадает под ограничения через регистрационные данные.

Для того чтобы было возможным подписывать данные с использованием механизмов подписи ГОСТ или RSA, необходимо иметь действующий сертификат RSA и регистрационные данные, позволяющие его использовать в данный момент времени. Регистрационные данные без ограничения по FSRAR_ID торговой точки подходят для использования совместно с любым действующим сертификатом RSA и служат для целей демонстрации функциональных возможностей Axiom Lab.

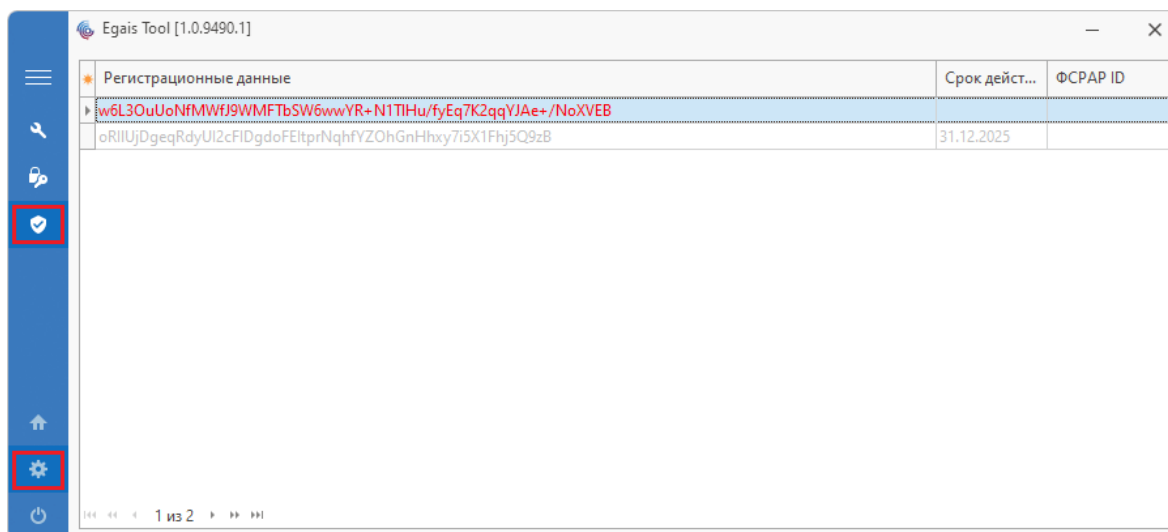
Регистрационные данные представляют собой строку в кодировке Base64. Для того чтобы внести те или иные регистрационные данные в Axiom Lab, необходимо скопировать их в буфер обмена, после чего вставить его содержимое в список раздела лицензирования утилиты конфигурирования.

После вставки содержимое буфера обмена, распознанное утилитой конфигурирования как корректные регистрационные данные Axiom Lab, отображается в специальном диалоге:



Список данного диалога динамичный – в него так же можно вставлять текст из буфера обмена (при этом список пополняется исключительно уникальными строками, распознанными как корректные регистрационные данные Axiom Lab), из него можно удалять неактуальные регистрационные данные. Все операции с регистрационными данными списка осуществляются через его контекстное меню.

Утилита конфигурирования подсвечивает имеющиеся регистрационные данные в зависимости от их состояния:

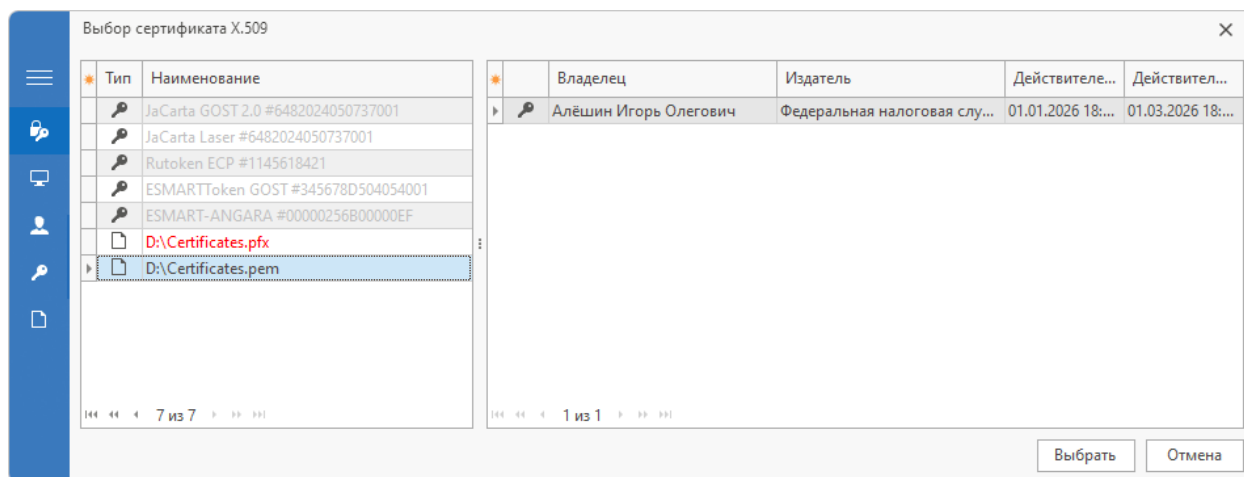


- **Красным** подсвечиваются строки, не распознанные как корректные регистрационные данные Axiom Lab
- **Серым** подсвечиваются неактуальные регистрационные данные, срок действия которых уже истек или еще не наступил

Все операции с регистрационными данными осуществляются через контекстное меню списка раздела лицензирования утилиты конфигурирования.

Сертификаты ГОСТ и RSA

При настройке Axiom Lab через утилиту конфигурирования достаточно часто (например, при создании или редактировании организаций и торговых точек) требуется выбирать сертификаты ГОСТ или RSA. Выбор сертификатов осуществляется через специальный диалог:



Диалог разбит на два списка, связанных отношением "мастер-деталь". Основной (мастер) список содержит множество доступных хранилищ сертификатов. Подчиненный (деталь) список содержит перечень сертификатов, содержащихся в выбранном хранилище.

Панель навигации диалога позволяет переключаться между источниками хранилищ сертификатов:

- Зарегистрированные [хранилища сертификатов](#)
- Системные хранилища сертификатов в контексте компьютера
- Системные хранилища сертификатов в контексте текущего пользователя
- Аппаратные ключи
- Файловые хранилища

Утилита конфигурирования подсвечивает хранилища сертификатов в зависимости от их состояния:

- **Красным** подсвечиваются недоступные хранилища сертификатов (для доступа к ним требуется указать секрет, т.е. пароль или пин-код)
- **Серым** подсвечиваются физически отсутствующие хранилища сертификатов (зарегистрированные, но изъятые аппаратные ключи или удаленные файлы), а также неактуальные сертификаты, срок действия которых уже истек или еще не наступил

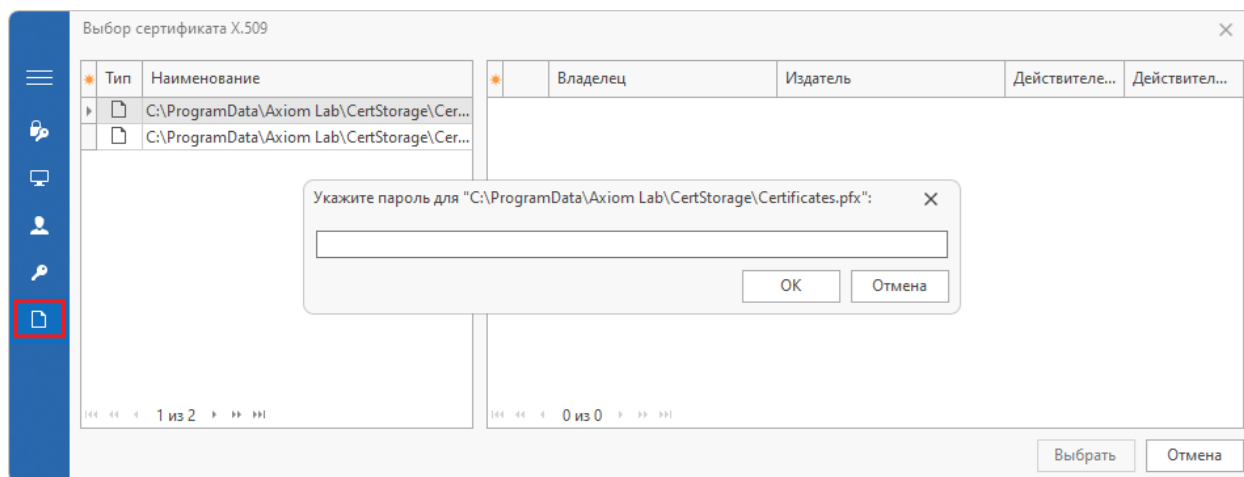
Логика выбора сертификата проста:

1. Понять, где располагается нужный сертификат и переключиться на соответствующий источник (начальным источником служат зарегистрированные хранилища сертификатов, что позволяет не указывать секрет для доступа к хранилищам)

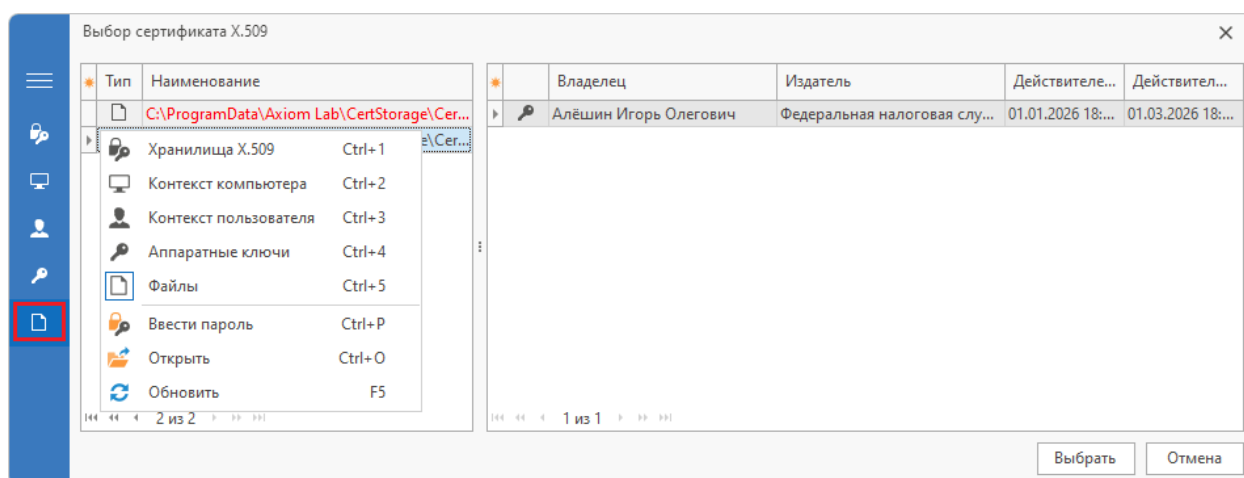
По умолчанию УТМ функционирует от имени системной учетной записи (Local System), в то время как утилита конфигурирования запускается самим пользователем. Выбор сертификатов для работы с УТМ из системных хранилищ сертификатов в контексте текущего пользователя приведет к тому, что УТМ

не сможет функционировать (или даже вовсе не запустится) по причине отсутствия сертификата, т.к. текущим пользователем для УТМ является системная учетная запись, а не сам пользователь.

- После того, как построится список хранилищ, выбрать нужное хранилище. Если хранилище сертификатов недоступно, утилита конфигурирования предложит ввести для него секрет:



Если источником являются файловые хранилища, в список включаются файлы поддерживаемых типов (JKS, PEM, PFX) из директории хранения файлов сертификатов с учетом [соответствующих настроек](#). Контекстное меню списка хранилищ позволяет дополнять его файлами любого из поддерживаемых типов:



Для работы с файловыми хранилищами сертификатов требуется наличие OpenSSL с движком ГОСТ.

- После того, как построится список сертификатов выбранного хранилища, найти в списке нужный и выбрать его.

В список сертификатов попадают не все сертификаты выбранного хранилища, а только те, что соответствуют критериям отбора. Таких критериев может быть несколько:

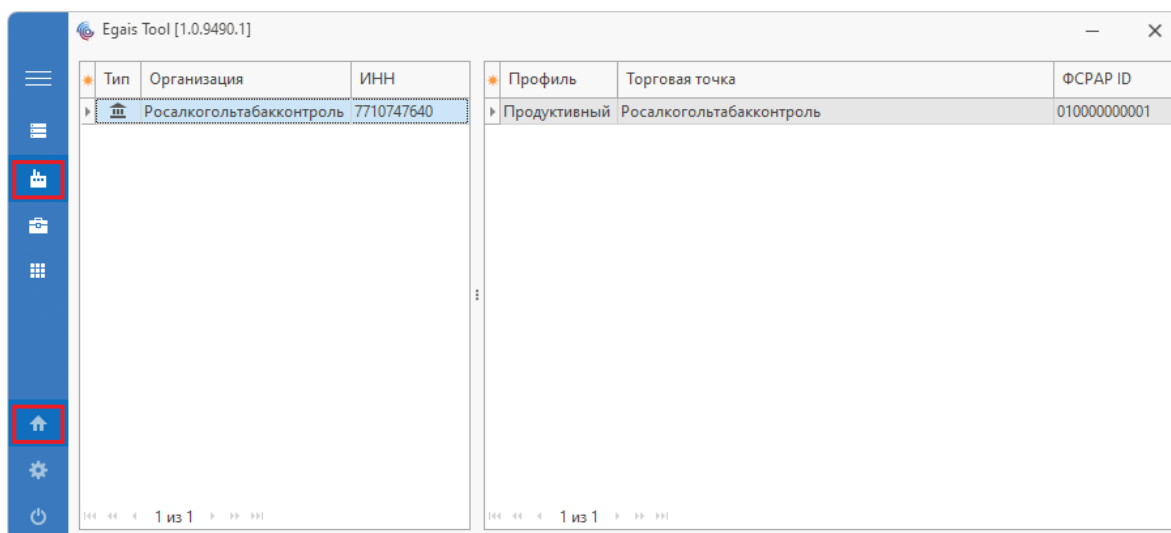
- При выборе сертификата ГОСТ в список включаются исключительно сертификаты ГОСТ и только они (имеющиеся сертификаты RSA в список не включаются)
- При выборе сертификата RSA в список включаются исключительно сертификаты RSA и только они (имеющиеся сертификаты ГОСТ в список не включаются)

- При выборе сертификата ГОСТ организации во время ее редактирования (ИНН организации уже определен и неизменен) в список включаются сертификаты юридических лиц и индивидуальных предпринимателей с соответствующим значением атрибута ИНН, а также сертификаты КЭП физических лиц для дальнейшего применения [МЧД](#)
- При выборе сертификата RSA торговой точки в список включаются сертификаты того контура ЕГАИС ([продуктивный](#) или [тестовый](#)), что и профиль УТМ торговой точки. Кроме того, сертификаты фильтруются по соответствию значения атрибута ИНН (если такой атрибут есть) значению ИНН организации

Данные критерии призваны сократить количество отображаемых сертификатов для того, чтобы свести к минимуму возможные ошибки.

Справочник организаций

Справочник организаций и торговых точек представляет собой представление отношения списка организаций и списка торговых точек, построенное по принципу "мастер-деталь":



В данном представлении основным (мастер) является расположенный слева список организаций, подчиненным (деталь) – расположенный справа список торговых точек. Список торговых точек отображает торговые точки выбранной организации и только их. Вывести в одно представление все торговые точки всех организаций нельзя.

Организация представляет собой запись со своим наименованием и уникальным ИНН (что позволяет избежать дублирование записей). Каждой организации можно указать сертификат ГОСТ.

Торговая точка представляет собой дочернюю по отношению к организации запись со своим наименованием, значением профиля УТМ и уникальным в его разрезе значением FSRAR_ID. Каждой торговой точке можно указать сертификат RSA. Каждая торговая точка может иметь отдельную директорию для хранения транспортной базы УТМ.

Уникальность FSRAR_ID в разрезе профилей УТМ позволяет избежать дублирование записей, при этом давая возможность иметь отдельные записи (со своими собственными транспортными базами УТМ) как для продуктивного контура ЕГАИС, так и для тестового.

Утилита конфигурирования подсвечивает организации и торговые точки в зависимости от их состояния:

- Серым подсвечиваются организации без сертификата ГОСТ, а также торговые точки без сертификата RSA

Контекстные меню списков организаций и торговых точек открывают доступ к выполнению операций над записями – добавление, редактирование и удаление. Там же доступна загрузка торговых точек из ЕГАИС.

Добавление организации

При добавлении организации необходимо указать ее наименование и уникальное значение ИНН:



В том случае, когда какой-либо из атрибутов организации будет иметь некорректное с точки зрения утилиты конфигурирования значение, соответствующее поле будет отмечено сигнализирующим о наличии ошибки знаком:

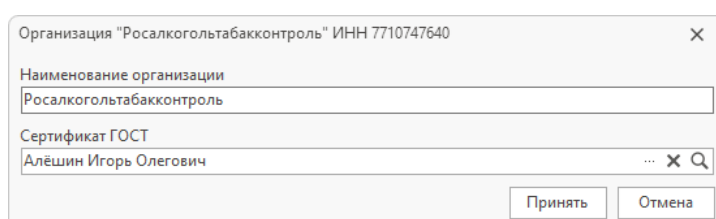


При необходимости имеется возможность [выбрать сертификат ГОСТ](#) организации – именно он будет использоваться в работе УТМ всех торговых точек организации.

Значение атрибута ИНН сертификата ГОСТ организации должно соответствовать значению ИНН организации. Исключением является использование в качестве сертификата ГОСТ сертификата КЭП физического лица для дальнейшего применением [МЧД](#), выданной этому физическому лицу данной организацией.

Редактирование организации

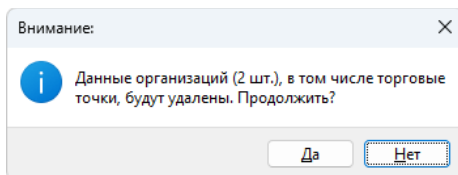
При редактировании организации имеется возможность изменить ее наименование и сертификат ГОСТ. Значение ИНН организации не подлежит редактированию:



В остальном функционал диалога редактирования организации идентичен функционалу диалога добавления организации.

Удаление организаций

Утилита конфигурирования позволяет удалять одну или несколько выбранных организаций вместе со всеми относящимися к ним торговыми точками. При получении утвердительного ответа на вопрос



утилита конфигурирования удаляет соответствующие записи без возможности их восстановления.

Удаление организаций и, следовательно, торговых точек влечет обнуление ссылок на них для всех реплик УТМ, если таковые ссылки имеются, что делает невозможным дальнейшее функционирование соответствующих УТМ (после их перезапуска).

Добавление торговой точки

При добавлении торговой точки организации необходимо указать ее наименование, выбрать профиль УТМ и указать FSRAR_ID торговой точки (при необходимости – директорию хранения ее транспортной базы УТМ):

Как отмечалось [ранее](#), комбинация значений профиля УТМ и FSRAR_ID должна быть уникальной в разрезе организации.

В том случае, когда какой-либо из атрибутов торговой точки будет иметь некорректное с точки зрения утилиты конфигурирования значение, соответствующее поле будет отмечено сигнализирующим о наличии ошибки знаком:

При добавлении торговой точки, не зарегистрированной в ЕГАИС (не имеющей своего FSRAR_ID) значение FSRAR_ID может быть пустым. Это необходимо для того, чтобы иметь возможность запустить УТМ с использованием одного лишь сертификата ГОСТ (без сертификата RSA).

При необходимости имеется возможность [выбрать сертификат RSA](#) – именно он будет использоваться в работе УТМ торговой точки.

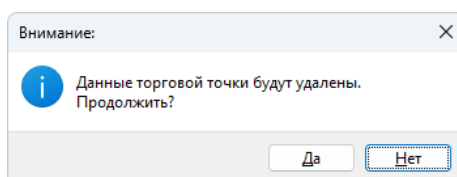
Значение атрибута CN сертификата RSA (значение FSRAR_ID) торговой точки должно соответствовать значению FSRAR_ID торговой точки.

Редактирование торговой точки

При редактировании торговой точки имеется возможность изменить значение любого ее атрибута. В остальном функционал диалога редактирования торговой точки идентичен функционалу диалога добавления торговой точки.

Удаление торговых точек

Утилита конфигурирования позволяет удалять одну или несколько выбранных торговых точек. При получении утвердительного ответа на вопрос

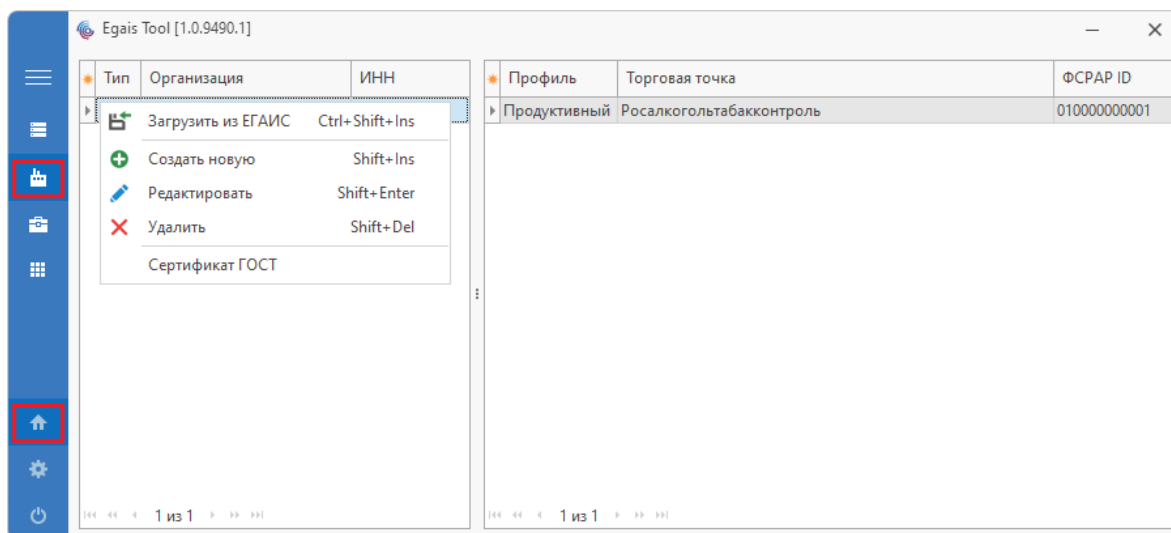


утилита конфигурирования удаляет соответствующие записи без возможности их восстановления.

Удаление торговых точек влечет обнуление ссылок на них для всех реплик УТМ, если таковые ссылки имеются, что делает невозможным дальнейшее функционирование соответствующих УТМ (после их перезапуска).

Загрузка торговых точек из ЕГАИС

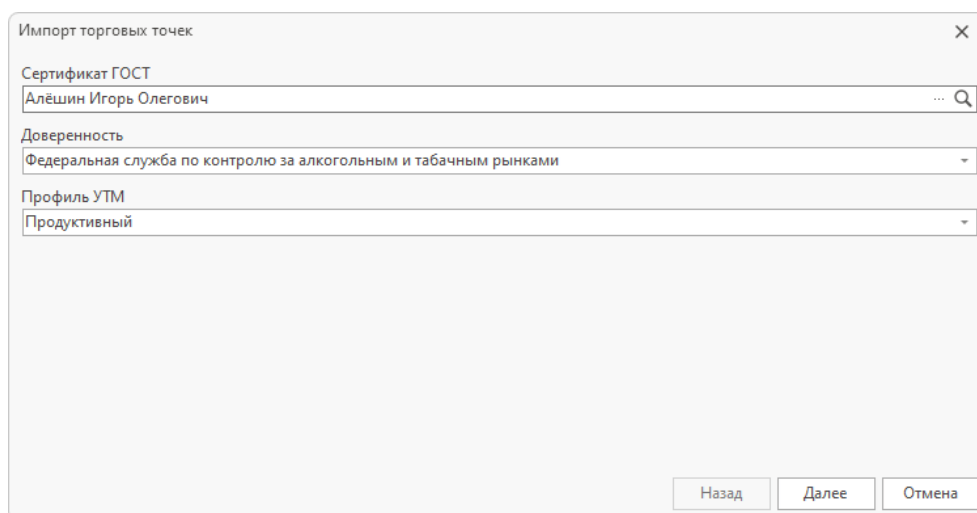
Утилита конфигурирования позволяет загружать торговые точки (и при необходимости на их основе создавать организации) непосредственно из ЕГАИС (с автоматическим созданием соответствующих сертификатов RSA):



Для загрузки торговых точек из ЕГАИС (получение списка торговых точек, формирование сертификата RSA торговой точки), требуется наличие OpenSSL.

Загрузка торговых точек производится в специальном диалоге и разбита на несколько шагов.

Шаг 1. Выбор сертификата ГОСТ организации и профиля УТМ торговых точек



На данном шаге необходимо [выбрать сертификат ГОСТ](#) организации, торговые точки которой должны быть загружены. Допускается выбор сертификата КЭП физического лица – в этом случае потребуется выбрать [МЧД](#), выданную организацией этому физическому лицу.

Через выбор профиля УТМ на данном шаге указывается контур ЕГАИС, из которого далее будет запрашиваться список торговых точек организации.

Для работы с сертификатами, хранящимися в файлах, требуется наличие OpenSSL с движком ГОСТ.

Шаг 2. Выбор торговых точек для дальнейшей загрузки

Импорт торговых точек

ФСРАР ID	Наименование	ИНН	КПП	Адрес
010000000001	РОСАЛКОГОЛЬРЕГУЛИРОВАНИЕ	7710747640	771001001	Россия, 125047, МОСКВА ГОРОД МИУССКАЯ...

1 из 1

Назад Далее Отмена

На данном шаге происходит обращение к выбранному ранее контуру ЕГАИС и запрашивается список торговых точек выбранной (через сертификат ГОСТ организации или [МЧД](#) физического лица) организации. Полученный список выводится в диалог. Выделенные в списке торговые точки подлежат дальнейшей загрузке.

Шаг 3. Выбор хранилища сертификата RSA

Импорт торговых точек

Вид хранилища сертификатов RSA

Файл сертификатов

Файл сертификатов

C:\ProgramData\Axiom Lab\CertStorage\Certificates.jks

Пароль

Пароль для ключей

Назад Далее Отмена

Для того чтобы загруженная торговая точка могла использоваться в УТМ, ей необходим сертификат RSA. При загрузке торговых точек утилита конфигурирования старается каждую из них обеспечить соответствующим сертификатом – использовать уже существующий или сформировать новый. Поиск и формирование сертификатов RSA осуществляется в хранилище сертификатов, выбираемом на данном шаге.

В зависимости от того, какое хранилище сертификатов было выбрано, имеется возможность указать секрет (пароль или пин-код) для доступа к хранилищу и (или) пароль для ключей:

- Для доступа к хранилищу из списка зарегистрированных [хранилищ сертификатов](#) никакой секрет не указывается – он был указан при регистрации хранилища. В том случае, если хранилище является файлом JKS, имеется возможность указать пароль для работы с ключами сертификата

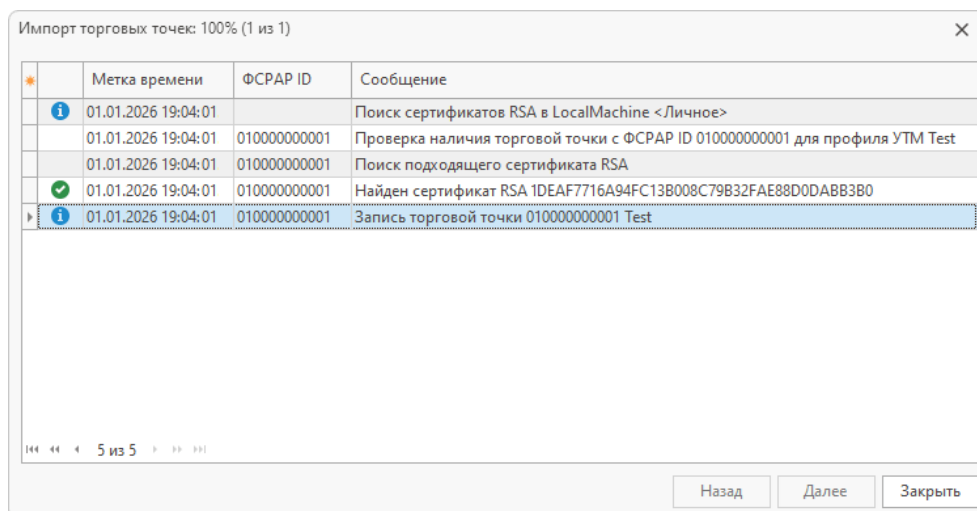
Файл JKS (Java Key Store) представляет собой хранилище сертификатов и закрытых ключей. Доступ к файлу осуществляется с использованием пароля, которым хранилище "запечатывается" – этот пароль никак не участвует в хранении закрытых ключей. Безопасное хранение закрытых ключей в хранилище обеспечивает лишь их шифрование с использованием пароля доступа к ключу.

В одном файле JKS (с общим паролем для доступа к хранилищу) может быть несколько сертификатов со своими закрытыми ключами. Каждый из ключей может храниться со своим собственным паролем.

- Для доступа к хранилищам, реализованным в виде аппаратных ключей, указывается пин-код
- Для доступа к хранилищам, реализованным в виде файлов, может указываться пароль. Для доступа к уже существующему файловому хранилищу, "запечатанному" с использованием какого-либо пароля, пароль обязателен. В том случае, если файловое хранилище еще не существует, оно будет создано и "запечатано" с использованием указанного пароля (в этом случае наличие пароля не обязательно, но рекомендовано). При этом:
 1. Для файлов PEM можно указать только пароль для ключей, т.к. для доступа к самому файлу пароль не требуется, а отдельные ключи могут быть зашифрованы каждый с использованием своего собственного пароля
 2. Для файлов JKS (JCEKS) можно указать пароль хранилища и пароль ключей
 3. Для файлов PKCS12 (PFX, P12) можно указать пароль хранилища

Для работы с файловыми хранилищами сертификатов требуется наличие OpenSSL с движком ГОСТ.

Шаг 4. Создание торговых точек



На данном шаге происходит создание торговых точек. Для каждой выбранной на шаге 2 записи выполняются следующие действия:

1. Проверка наличия соответствующей торговой точки в справочнике организаций с учетом профиля УТМ и значения FSRAR_ID. Если соответствующая торговая точка найдена, ее загрузка считается выполненной
2. Поиск подходящего по реквизитам (профиль УТМ, значение FSRAR_ID) сертификата RSA. Если соответствующий сертификат не найден, требуемый сертификат формируется через ЕГАИС

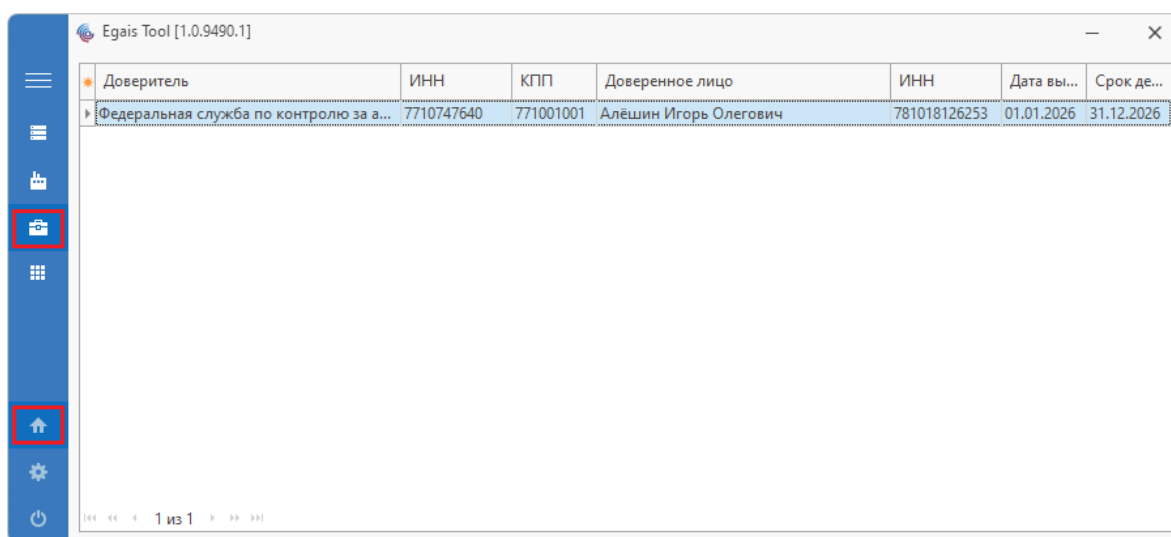
3. Запись торговой точки со ссылкой на сертификат RSA в справочник организаций

Загрузка торговых точек осуществляется в многопоточном режиме (одновременно загружаются несколько торговых точек). Все действия и их результаты журналируются с указанием метки времени и значения FSRAR_ID торговой точки.

Реестр МЧД

Для формирования сертификатов RSA с использованием сертификата КЭП физического лица необходимо использовать МЧД, выданную этому физическому лицу той или иной организацией.

МЧД представляет собой набор из двух файлов – XML файла данных доверенности и P7S (или SIG) файла подписи доверенности. Утилита конфигурирования позволяет вести реестр доверенностей:



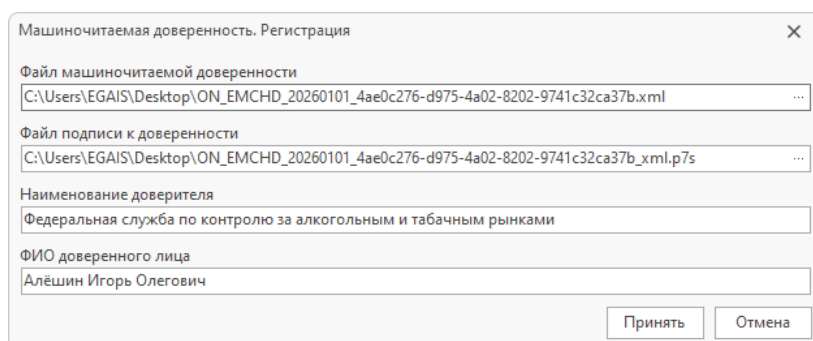
Утилита конфигурирования подсвечивает доверенности в зависимости от их состояния:

- Серым подсвечиваются неактуальные доверенности, срок действия которых уже истек или еще не наступил

Все операции с доверенностями осуществляются через контекстное меню списка реестра МЧД утилиты конфигурирования.

Регистрация МЧД

Регистрация машиночитаемых доверенностей производится в специальном диалоге:



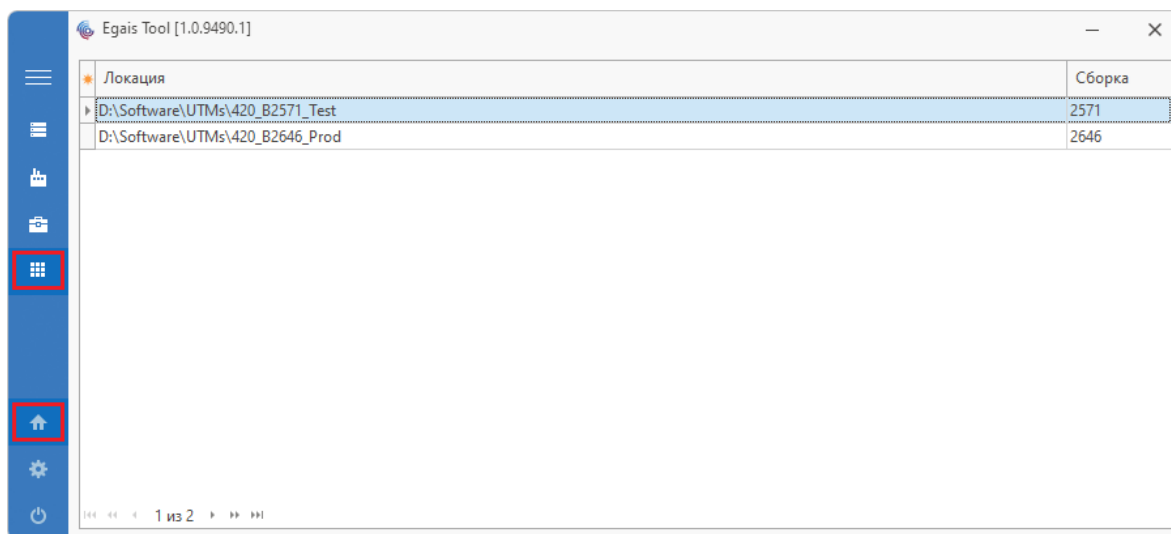
При регистрации МЧД требуется выбрать XML файл данных доверенности и соответствующий ему P7S (или SIG) файл подписи доверенности (при наличии подходящего файла в директории, содержащей XML файл данных доверенности, он "выбирается" автоматически). Утилита конфигурирования разбирает данные доверенности и выводит их в диалог для того, чтобы было возможным понять, какая именно доверенность была выбрана.

Данные подписи доверенности используются исключительно при загрузке торговых точек из ЕГАИС и никак не проверяются при регистрации доверенности. Считается, что доверенность действительна и валидна.

После регистрации файлы доверенности и ее подписи сохраняются в базе данных Axiom Lab и в целом больше не нужны.

Версии УТМ

Как правило, УТМ устанавливается в единственном экземпляре в директорию "C:\UTM", что не дает возможность как одновременного использования различных версий УТМ, так и переключения УТМ с одной версии на другую без потери данных и времени. Утилита конфигурирования решает обе эти проблемы.



Утилита конфигурирования подсвечивает версии УТМ в зависимости от их состояния:

- Серым подсвечиваются физически отсутствующие версии УТМ

Все операции с версиями УТМ осуществляются через контекстное меню списка версий УТМ утилиты конфигурирования.

Регистрация версий УТМ

Для регистрации какой-либо версии УТМ требуется иметь ее копию в отдельной директории (чтобы избежать ее случайного удаления при деинсталляции УТМ).

После установки УТМ рекомендуется создавать его копию в отдельной директории (с включением в ее имя версии и номера сборки УТМ).

При регистрации какой-либо версии УТМ запрашивается путь к директории, содержащей эту версию. Утилита конфигурирования проверяет

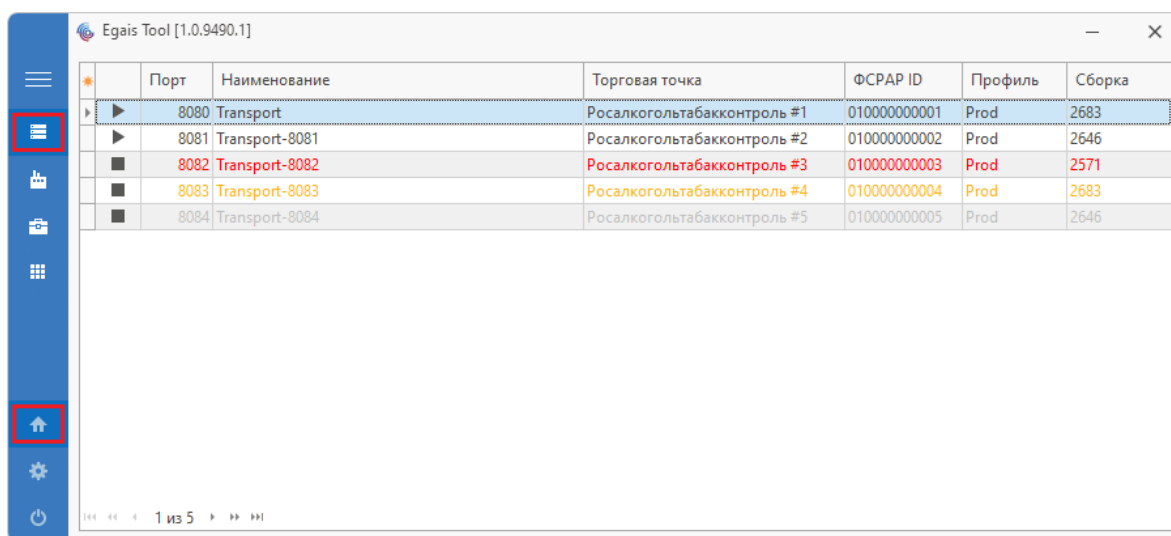
1. Корректность указанного пути. При наличии в пути запрещенных символов (включая пробел) выдается соответствующее сообщение
2. Наличие обязательных для УТМ крайних версий (сборки УТМ версии 4.20) артефактов (файлов в определенных поддиректориях). При отсутствии какого-либо обязательного артефакта выдается соответствующее сообщение

После того как утилита конфигурирования убедится в корректности предоставленной версии УТМ, она получает номер его сборки и сохраняет запись в базе данных Axiom Lab.

Управление УТМ

Утилита конфигурирования предоставляет достаточно богатый функционал по администрированию УТМ. Она позволяет:

- Реплицировать УТМ любой из [зарегистрированных версий](#), позволяя всем репликам работать одновременно (при условии достаточности ресурсов CPU и RAM)
- Быстро переключать реплики УТМ с одной версии на другую без потери данных
- Изменять тип запуска транспортных сервисов УТМ, в т.ч. отключать их запуск
- Запускать и останавливать транспортные сервисы УТМ вручную
- Настраивать параметры прокси для транспортных сервисов УТМ
- Открывать домашние страницы УТМ в браузере



	Порт	Наименование	Торговая точка	ФСРАР ID	Профиль	Сборка
▶	8080	Transport	Росалкогольтабакконтроль #1	010000000001	Prod	2683
▶	8081	Transport-8081	Росалкогольтабакконтроль #2	010000000002	Prod	2646
■	8082	Transport-8082	Росалкогольтабакконтроль #3	010000000003	Prod	2571
■	8083	Transport-8083	Росалкогольтабакконтроль #4	010000000004	Prod	2683
■	8084	Transport-8084	Росалкогольтабакконтроль #5	010000000005	Prod	2646

Список реплик УТМ отображает статус каждого транспортного сервиса в виде пиктограммы. Помимо этого, он содержит сведения о номере порта и наименовании транспортного сервиса, наименовании и значении FSRAR_ID соответствующей торговой точки, профиле и номере сборки УТМ.

Утилита конфигурирования подсвечивает реплики УТМ в зависимости от их состояния:

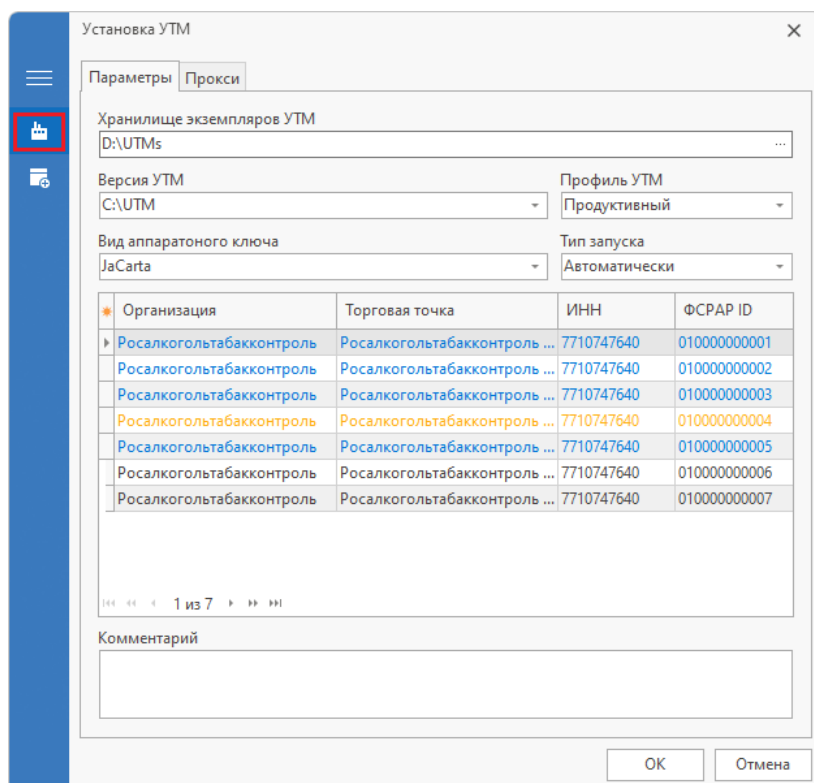
- **Красным** подсвечиваются реплики, состояние которых делает невозможным использование УТМ:
 1. Соответствующий транспортный сервис каким-либо образом был удален без фиксации данного факта в утилите конфигурирования и в настоящий момент недоступен
 2. Отсутствуют [регистрационные данные](#), позволяющие в текущий момент времени использовать сертификаты соответствующей торговой точки
 3. Организация соответствующей торговой точка не содержит сведений о сертификате ГОСТ
- **Оранжевым** подсвечиваются реплики, торговая точка которых не содержит сведений о сертификате RSA
- **Серым** подсвечиваются реплики, транспортный сервис которых отключен

Все операции с репликами УТМ осуществляются через контекстное меню списка реплик УТМ утилиты конфигурирования.

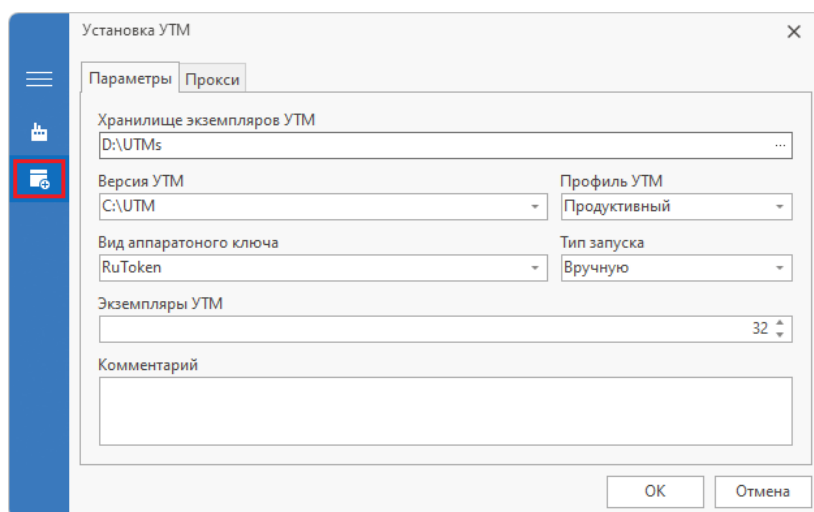
Создание реплик УТМ

Создание реплик УТМ производится в специальном диалоге. Диалог имеет панель навигации, дающую возможность переключения между двумя режимами создания реплик УТМ:

- Создание реплик УТМ по имеющимся торговым точкам



- Создание требуемого количества реплик УТМ без указания торговых точек (каждой реплике торговую точку можно задать отдельно)



Для создания реплик УТМ (вне зависимости от выбранного режима реплицирования), требуется:

1. Указать хранилище экземпляров УТМ – директорию, в которой будут создаваться директории хранения состояния транспортного сервиса УТМ. Данный параметр подлежит [настройке](#)
2. Выбрать [версию УТМ](#), на базе которой будут создаваться реплики
3. Выбрать профиль УТМ ([продуктивный](#) или [тестовый](#)) создаваемых реплик
4. Выбрать вид аппаратного ключа Axiom Lab для функционирования создаваемых реплик

Axiom Lab реализует модели аппаратных ключей RuToken и JaCarta. Для функционирования УТМ можно использовать любую из моделей (вне зависимости от психологических предпочтений, основанных на удачном или не очень удачном опыте использования физических аппаратных ключей).

Поскольку для корректного функционирования УТМ с использованием аппаратных ключей RuToken (ровно, как и ESmart и MS Key K) требуется два экземпляра библиотеки для работы с аппаратными ключами через интерфейс PKCS#11 (ну, не научились разработчики УТМ работать с одним апплетом аппаратного ключа в разных логически изолированных объектах, обеспечивающих взаимодействие с ключами ГОСТ и RSA), в то время как для аппаратных ключей JaCarta – всего один (в силу того, что аппаратный ключ JaCarta-2 PKI/ГОСТ комбинированный и содержит два независимых друг от друга апплета – один для ключей ГОСТ, второй – для ключей RSA, что допускает их использование в разных логически изолированных объектах), предпочтительным является использование ключей [JaCarta](#).

5. Выбрать тип запуска транспортного сервиса создаваемых реплик

Как правило, достаточно автоматического запуска транспортных сервисов – в этом случае все они будут стартовать после загрузки операционной системы (возможно, излишне ее нагружая). В случае, когда автоматический запуск транспортных сервисов нежелателен, можно выбрать иной вариант.

Создание реплик УТМ по имеющимся торговым точкам

В данном режиме в списке торговых точек диалога выбираются торговые точки, для которых требуется создать отдельную реплику УТМ.

Список содержит только те торговые точки, у которых значение профиля УТМ совпадает со значением профиля УТМ в диалоге, что сокращает размер списка, упрощает выбор и не позволяет использовать сертификаты RSA тестового контура ЕГАИС для работы с продуктивным контуром и наоборот.

Утилита конфигурирования подсвечивает торговые точки в зависимости от их состояния:

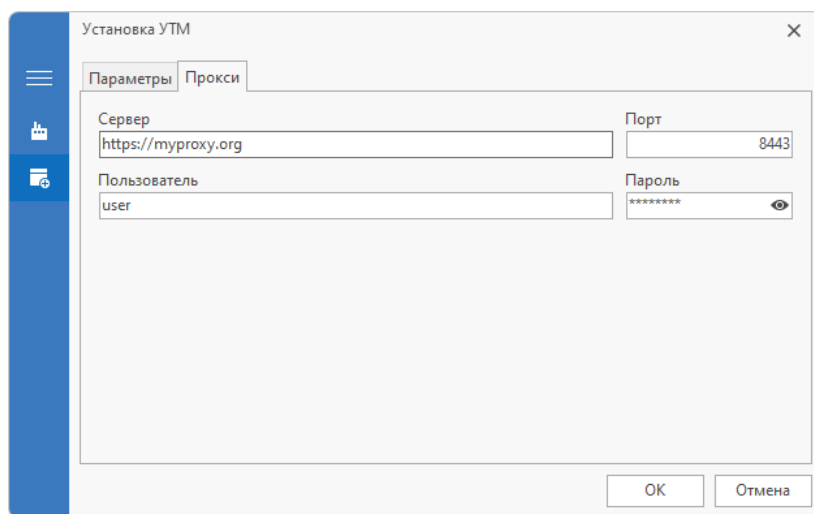
- **Синим** подсвечиваются торговые точки, уже задействованные в той или иной реплике УТМ. Повторное их использование в репликах УТМ не запрещено, но крайне нежелательно
- **Красным** подсвечиваются торговые точки, организации которых не содержащие сведений о сертификате ГОСТ
- **Оранжевым** подсвечиваются торговые точки, не содержащие сведений о сертификате RSA

Создание требуемого количества реплик УТМ

В данном режиме указывается количество экземпляров создаваемых реплик УТМ.

Параметры прокси реплик УТМ

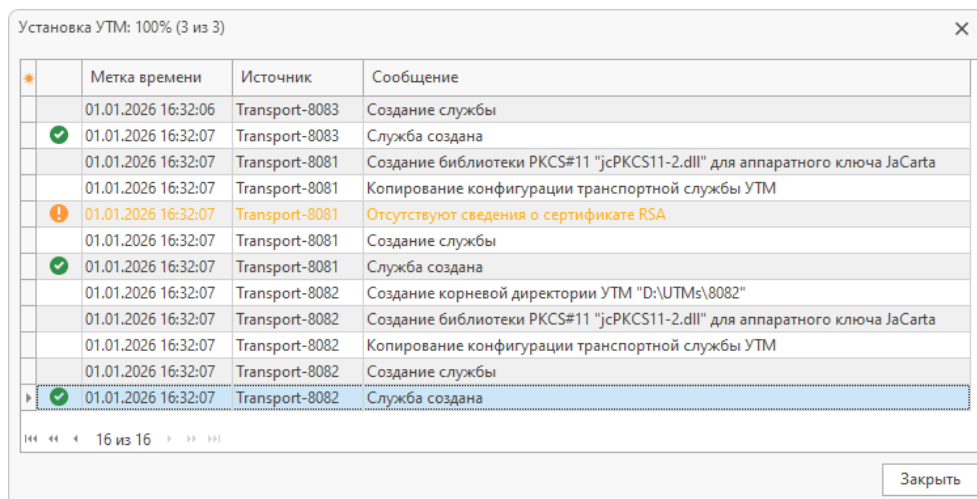
Конфигурация УТМ позволяет указывать параметры прокси (хост и номер порта сервиса, а также имя пользователя и пароль для доступа к нему) для транспортного сервиса УТМ. Утилита конфигурирования позволяет задать данные параметры на еще этапе создания реплик УТМ:



После проверки (успешной попытки подключения) указанные значения будут прописаны в файле конфигурации ("transport.properties") каждой создаваемой реплики УТМ.

Установка УТМ

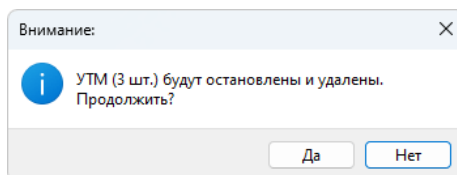
При принятии параметров диалога (нажатии кнопки "ОК") утилита конфигурирования начинает реплицирование УТМ. Создание реплик осуществляется в многопоточном режиме (одновременно создаются несколько реплик). Все действия и их результаты журналируются с указанием метки времени и наименования транспортного сервиса создаваемой реплики УТМ:



При отсутствии сообщений, требующих внимания (предупреждения, ошибки), журнал автоматически закрывается после окончания репликации УТМ.

Удаление реплик УТМ

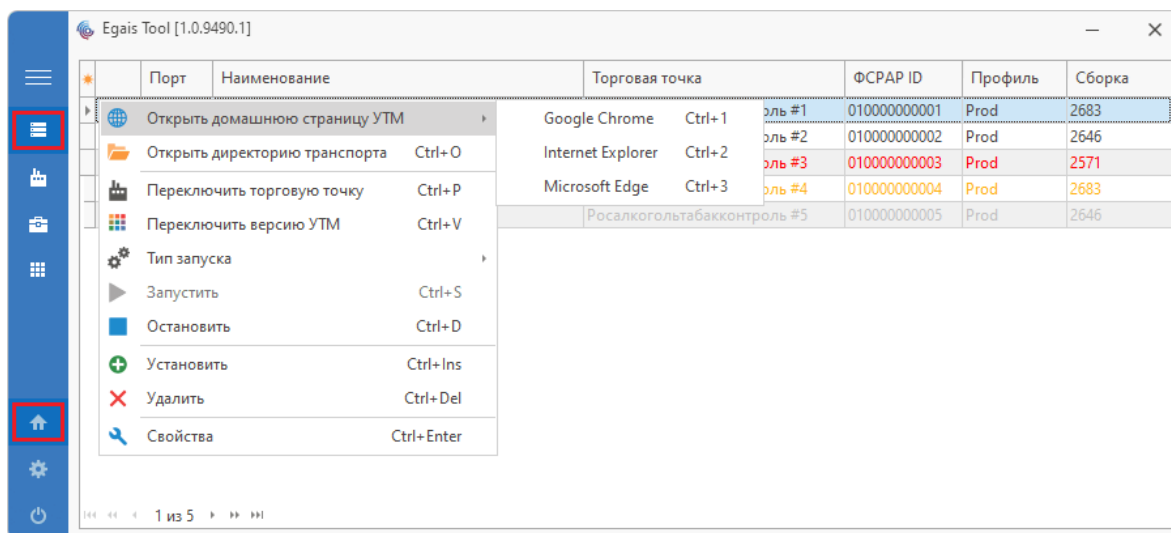
Утилита конфигурирования позволяет удалять одну или несколько выбранных реплик УТМ. При получении утвердительного ответа на вопрос



утилита конфигурирования останавливает и удаляет транспортные сервисы соответствующих реплик УТМ и удаляет соответствующие записи из базы данных без возможности их восстановления.

Домашние страницы УТМ

Утилита конфигурирования позволяет открыть домашнюю страницу выбранной реплики УТМ в любом из обнаруженных в системе браузеров через соответствующий браузеру подпункт пункта "Открыть домашнюю страницу УТМ" контекстного меню списка реплик УТМ:



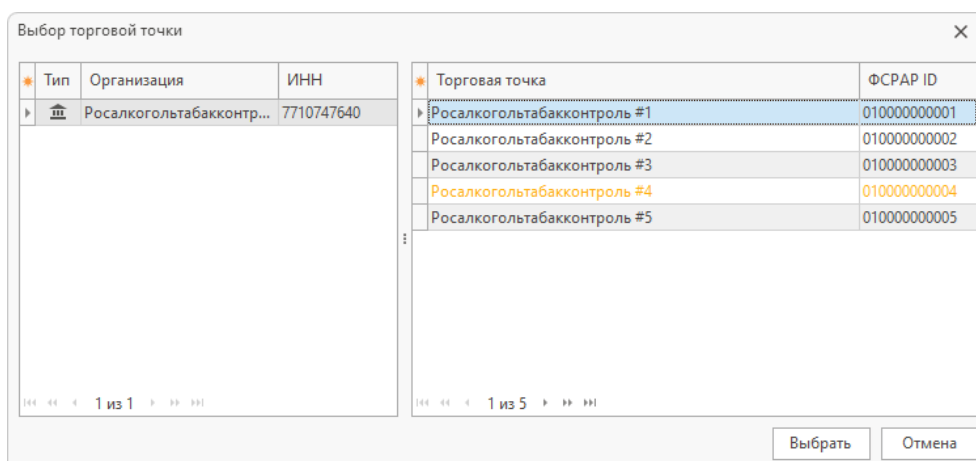
Директории транспорта

Утилита конфигурирования позволяет открыть директорию транспортного сервиса ("transporter") выбранной реплики УТМ в отдельной папке проводника Windows (Explorer) через пункт "Открыть директорию транспорта" контекстного меню списка реплик УТМ. Данная операция может быть полезной при необходимости проверить конфигурацию соответствующего транспортного сервиса, посмотреть его логи или убедиться в наличии транспортной базы УТМ.

Переключение торговой точки

Утилита конфигурирования позволяет переключить выбранную реплику УТМ с одной торговой точки на другую (либо настроить реплику УТМ на работу с той или иной торговой точкой в том случае, когда реплика не настроена ни на одну торговую точку) через пункт "Переключить торговую точку" контекстного меню списка реплик УТМ.

Для переключения (настройки) выбранной реплики УТМ на ту или иную торговую точку необходимо выбрать нужно торговую точку в специальном диалоге:



Список содержит только те торговые точки, у которых значение профиля УТМ совпадает со значением профиля выбранной реплики УТМ, что сокращает размер списка, упрощает выбор и не позволяет использовать сертификаты RSA тестового контура ЕГАИС для работы с продуктивным контуром и наоборот.

Утилита конфигурирования подсвечивает организации и торговые точки в зависимости от их состояния:

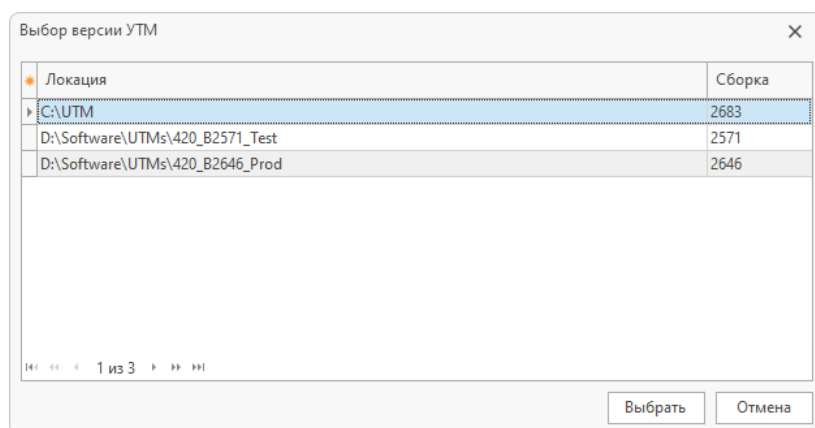
- **Красным** подсвечиваются организации, не содержащие сведений о сертификате ГОСТ
- **Оранжевым** подсвечиваются торговые точки, не содержащие сведений о сертификате RSA

Если исходная торговая точка выбранной реплики УТМ (та, на которую реплика была настроена до переключения) не имеет своей директории хранения транспортной базы УТМ, текущая транспортная база этой торговой точки (та, что в данный момент располагается в поддиректории "transportDB" директории "transporter" УТМ) удаляется, при этом хранящиеся в ней документы (как входящие, так и исходящие) теряются.

Переключение версии УТМ

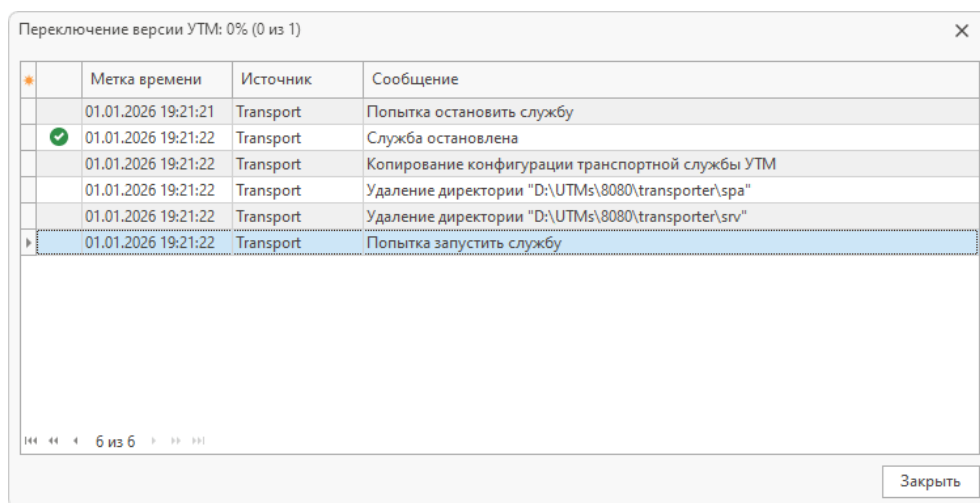
Утилита конфигурирования позволяет быстро переключить выбранные реплики УТМ с одной версии УТМ на другую через пункт "Переключить версию УТМ" контекстного меню списка реплик УТМ.

Для переключения выбранных реплик УТМ на ту или иную версию УТМ необходимо выбрать целевую версию УТМ в специальном диалоге:



Для каждой выбранной реплики УТМ выполняются следующие действия: остановка работающего транспортного сервиса, удаление чувствительных к версии УТМ директорий и запуск транспортного сервиса (если ранее тот был остановлен).

Переключение версии УТМ осуществляется в многопоточном режиме (одновременно обрабатывается несколько реплик УТМ). Все действия и их результаты журналируются с указанием метки времени и наименования транспортного сервиса создаваемой реплики:



Директории транспортных баз УТМ вместе со всеми хранящимися в них документами сохраняются в неизменном виде.

Изменение типа запуска сервисов

Утилита конфигурирования позволяет изменять тип запуска транспортных сервисов выбранных реплик УТМ через соответствующий подпункт пункта "Тип запуска" контекстного меню списка реплик УТМ.

Возможны следующие типы запуска сервисов:

- "Автоматически". Предполагает, что сервисы будут стартовать автоматически после загрузки операционной системы

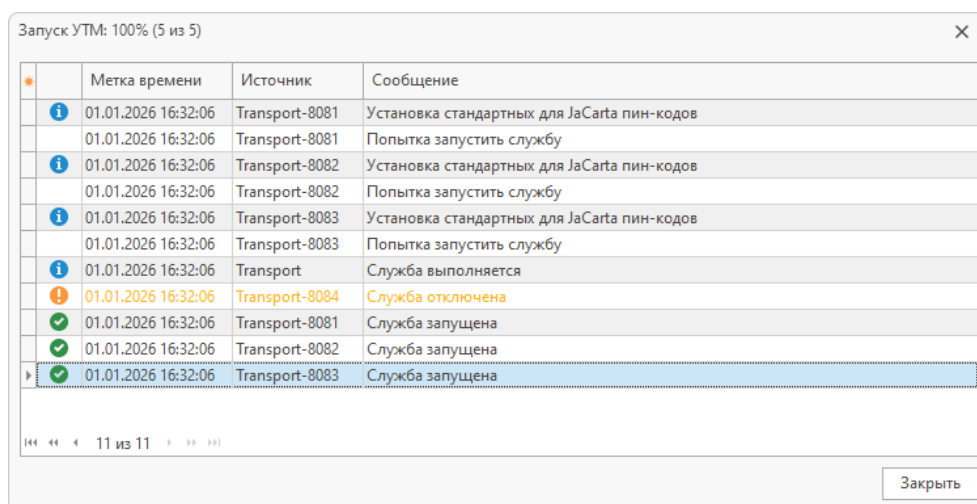
- "Вручную". Предполагает, что сервисы при необходимости можно запустить вручную
- "Отключен". Предполагает, что запуск сервисов невозможен вовсе

Запуск и остановка сервисов

Утилита конфигурирования позволяет по необходимости запускать и останавливать транспортные сервисы выбранных реплик УТМ через соответствующие пункты контекстного меню списка реплик УТМ:

- Для запуска транспортных сервисов служит пункт "Запустить"
- Для остановки транспортных сервисов служит пункт "Остановить"

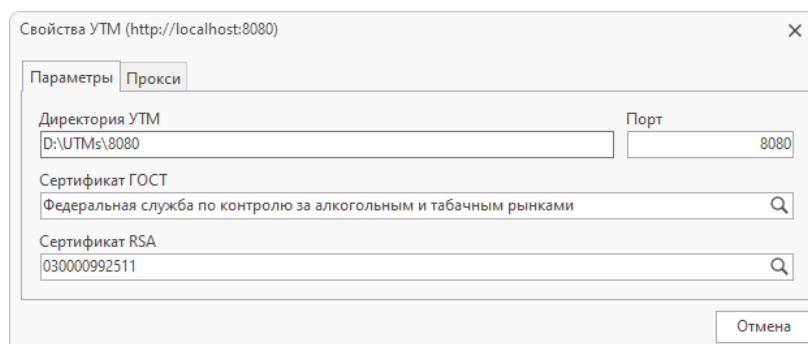
Запуск и остановка транспортных сервисов осуществляется в многопоточном режиме (одновременно обрабатывается несколько транспортных сервисов). Все действия и их результаты журналируются с указанием метки времени и наименования обрабатываемого транспортного сервиса УТМ:



Свойства реплик УТМ

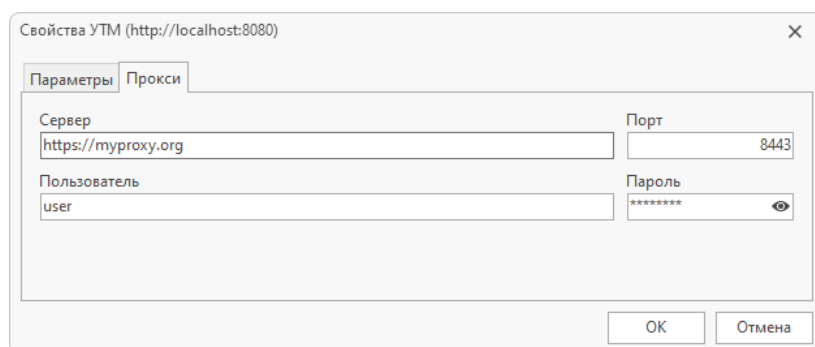
Утилита конфигурирования позволяет просмотреть параметры (директория хранения состояния и номер порта транспортного сервиса УТМ, используемые сертификаты ГОСТ и RSA, конфигурация прокси) выбранной реплики УТМ через пункт "Свойства" контекстного меню списка реплик УТМ.

Параметры реплики УТМ отображаются в специальном диалоге:



Все значения на вкладке "Параметры" данного диалога носят информационный характер и не редактируются.

Диалог позволяет просмотреть и при необходимости отредактировать конфигурацию прокси соответствующей реплики УТМ:



При принятии параметров прокси (нажатии кнопки "ОК") утилита конфигурирования проверяет введенные значения. После успешной попытки подключения значения прописываются в файле конфигурации ("transport.properties") реплики УТМ, а соответствующий транспортный сервис УТМ перезапускается. Все действия и их результаты журналируются с указанием метки времени и наименования транспортного сервиса УТМ.