Руководство по настройке терминала торговой системы с использованием ЭЦП

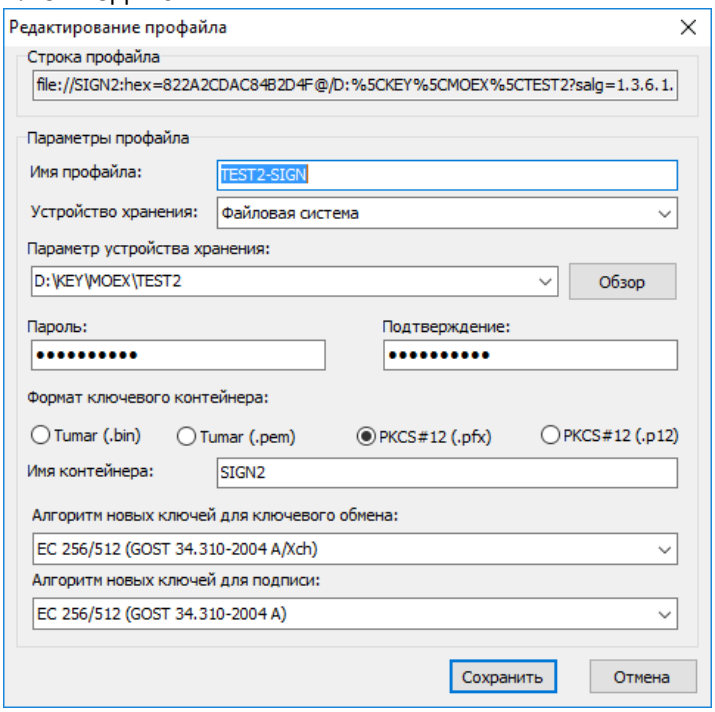
1. Установка ТУМАР-CSP

a) Скачать и установить последнюю версию криптоядра ТУМАР-CSP по адресу:

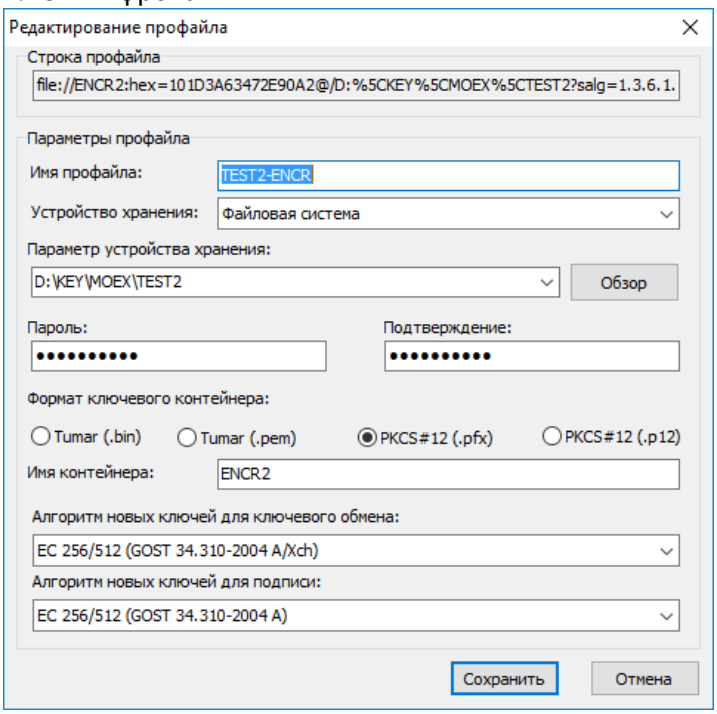
https://ca.kisc.kz/webra/res-open/client/TumarCSP.zip

b) Запустить утилиту “TumarCSP Configurator”, создать ключевой профайл для подписи и шифрования и загрузить в него ключ, например:

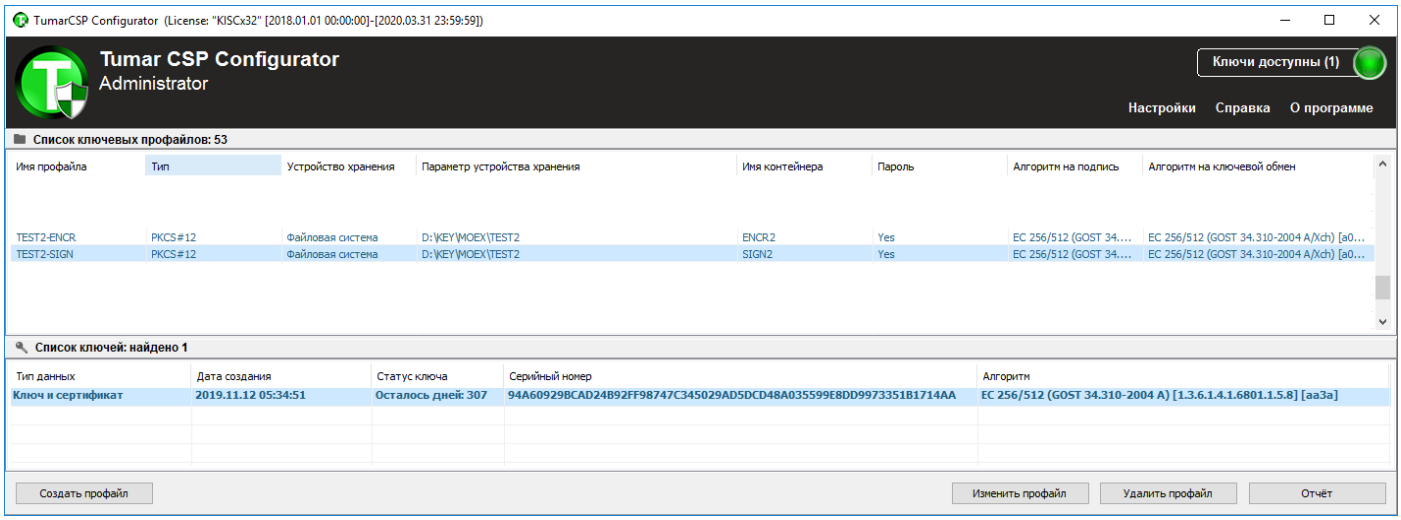
Ключ подписи



Ключ шифрования



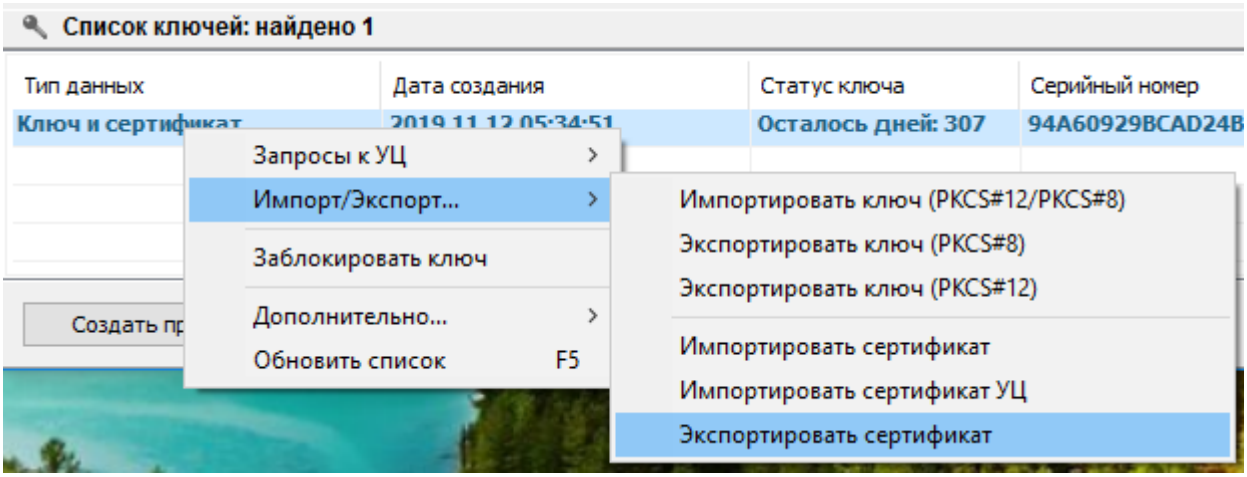
В случае корректной настройки, при выборе профайла должна светиться зеленая надпись «Ключи доступны (1)», а загруженный ключ отображаться в списке ключей:

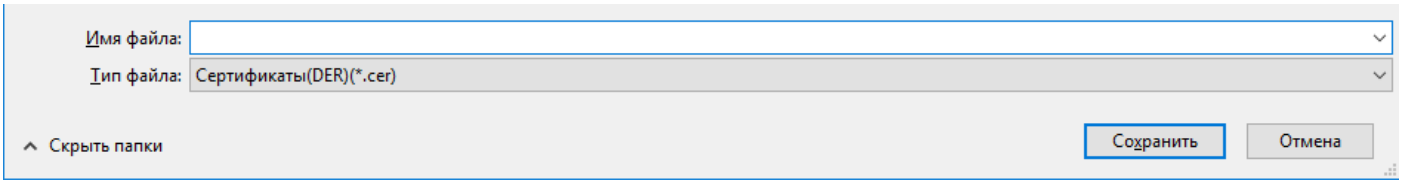


2. Формирование каталога с сертификатами

a) Создать временный пустой каталог с доступом на запись и чтение.

b) В контекстном меню окна «Список ключей» утилиты “TumarCSP Configurator” выбрать команду «Импорт/Экспорт...» -> “Экспортировать сертификат» и сохранить сертификат в кодировке DER в каталог, созданный на шаге 2a. Выполнить экспорт сертификата для ключа подписи и шифрования.





c) Скачать корневой сертификат УЦ КЦМР (алгоритм ГОСТ 34.310) в формате DER и список отозванных сертификатов (алгоритм ГОСТ 34.310) по адресу:

http://www.kisc.kz/catalog/udos-center/br/1019.html

Промышленный УЦ:

Корневое регистрационное свидетельство УЦ КЦМР. Алгоритм ГОСТ 34.310	**Серийный номер:** 1e 97 16 12 b3 4f 8d e4 e8 39 8b da 34 f5 1e f5 3f c6 0f b8 29 cf 7a 07 c0 7a db f5 9f e9 12 0b **Срок действия:** 2 сентября 2008 г. по 28 августа 2028 г. **sha1 отпечаток:** f3 97 7e b6 ca 40 ea 01 ce c2 91 41 78 4a d3 d0 7c 4a 93 da	Скачать в формате DER Скачать в формате PEM	Скачать список отозванных регистрационных свидетельств пользователей. Алгоритм ГОСТ 34.310

и сохранить их в каталог, созданный на шаге 2a.

Внимание: необходимо изменить расширение файла с сертификатом УЦ с «.CRT» на «.CER».

3. Установка ПК «Справочник сертификатов»

a) Скачать и установить последнюю версию ПК «Справочник сертификатов» (неквалифицированные сертификаты) по адресу:

http://kase.kz/ru/kase_moex_connection/ в разделе Trade SE (терминал торговой системы)

в зависимости от разрядности операционной системы (32 или 64 бита) выбрать один из двух вариантов:

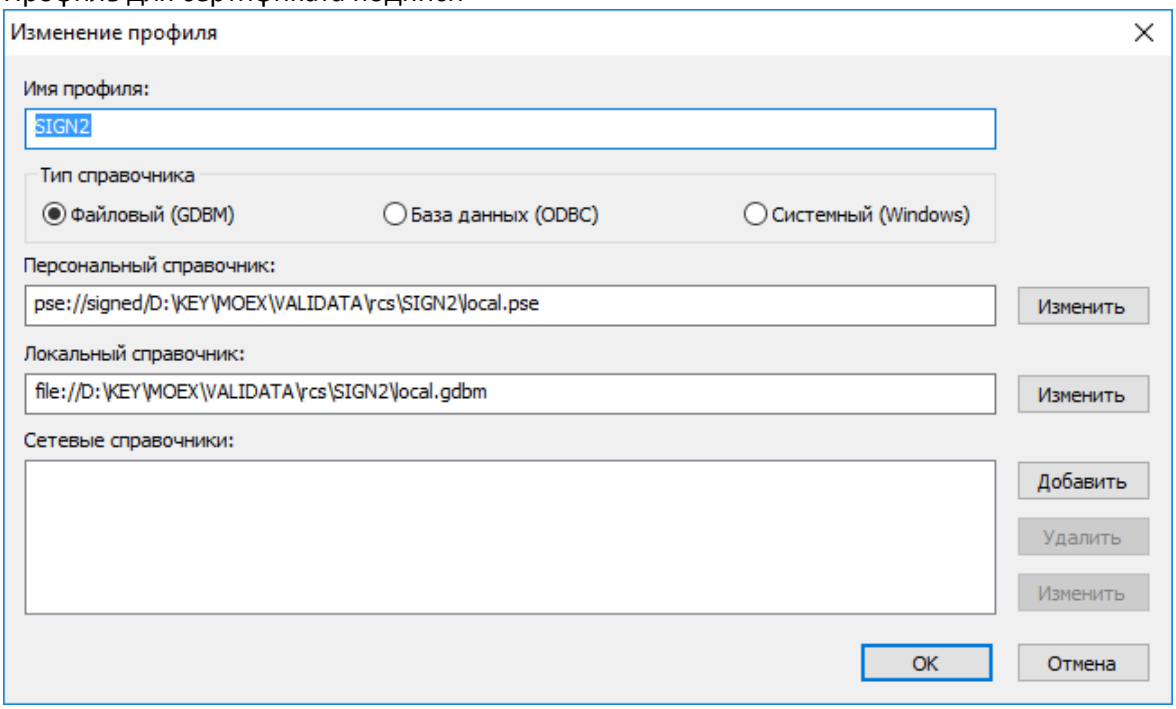
Программное обеспечение ПК "Справочник сертификатов" x64

Программное обеспечение ПК "Справочник сертификатов" x32

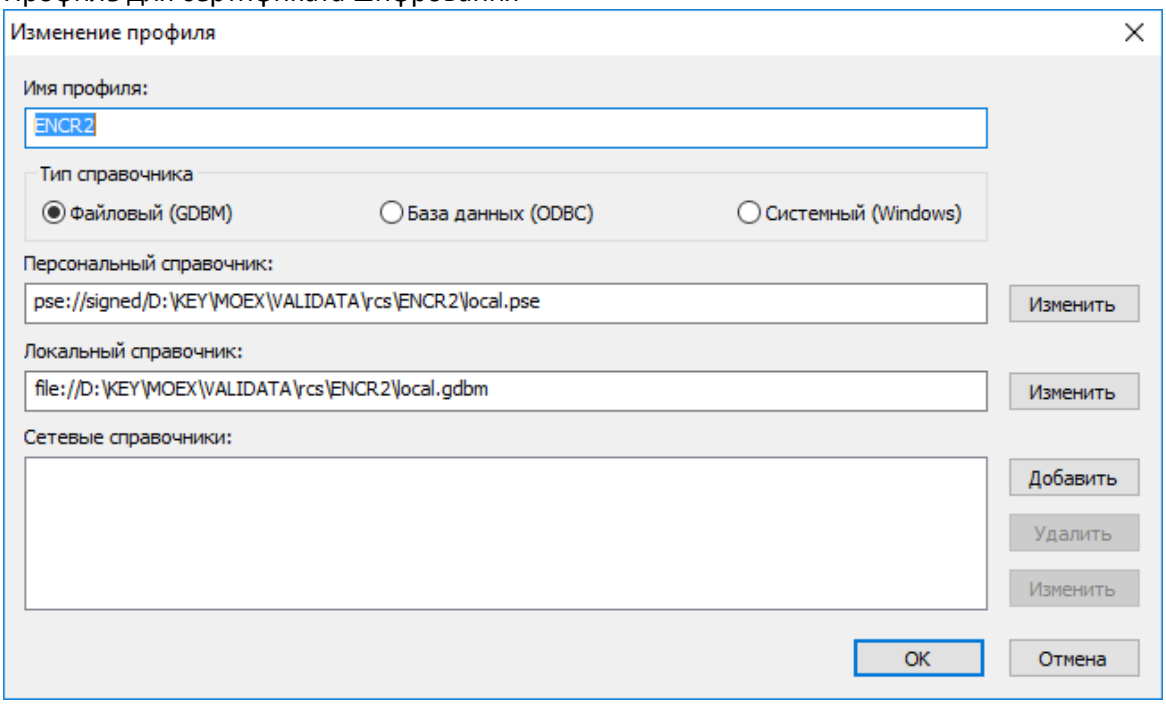
Можно установить оба дистрибутива, чтобы иметь возможность использовать криптоядро в ПО любой разрядности.

b) Запустить ПК «Справочник сертификатов» и создать два профиля, выбрав команду «Профили» -> «Настройка профилей» -> «Добавить». Задать имя профиля. Пути к персональному и локальному справочникам можно оставить по умолчанию. Все сетевые справочники необходимо удалить. Нажать «ОК» во всех окнах.

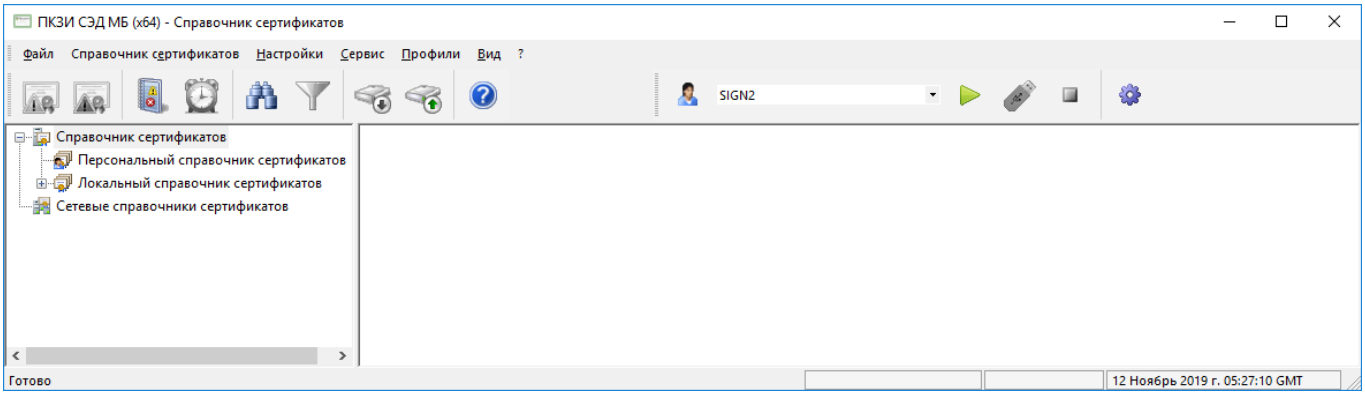
Профиль для сертификата подписи



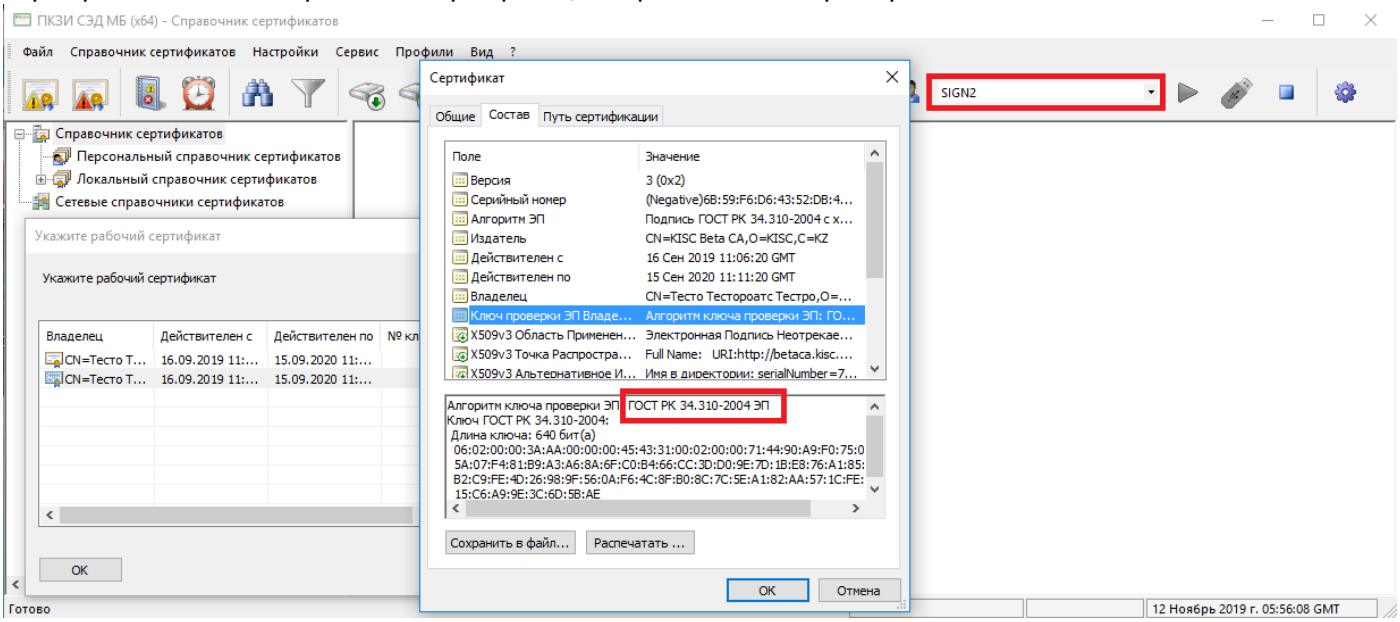
Профиль для сертификата шифрования

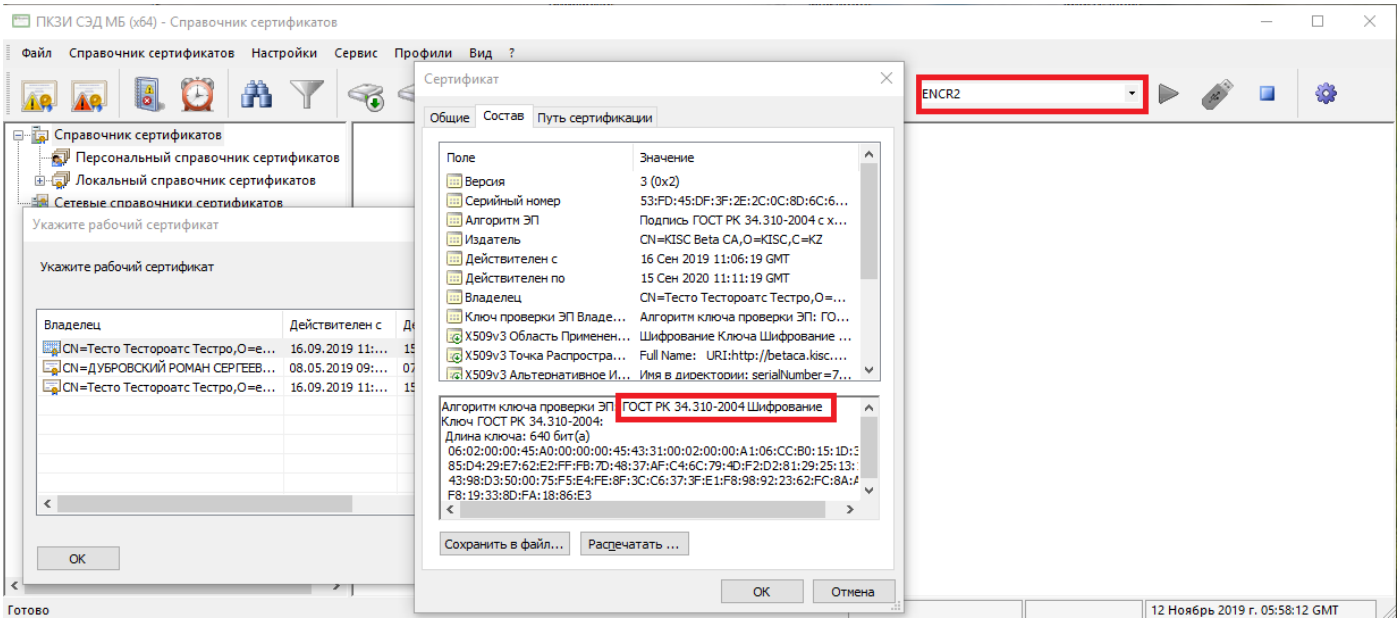


Выбрать созданный профиль в выпадающем списке профилей в панели инструментов и нажать кнопку «Загрузить профиль» (зеленый треугольник):



c) Выбрать команду «Сервис» -> «Сформировать справочник из каталога», указать каталог, в который на шаге 2а были сохранены собственный сертификат, сертификат УЦ КЦМР и список отозванных сертификатов. Указать рабочий сертификат, выбрать контейнер закрытого ключа ТУМАР-CSP.

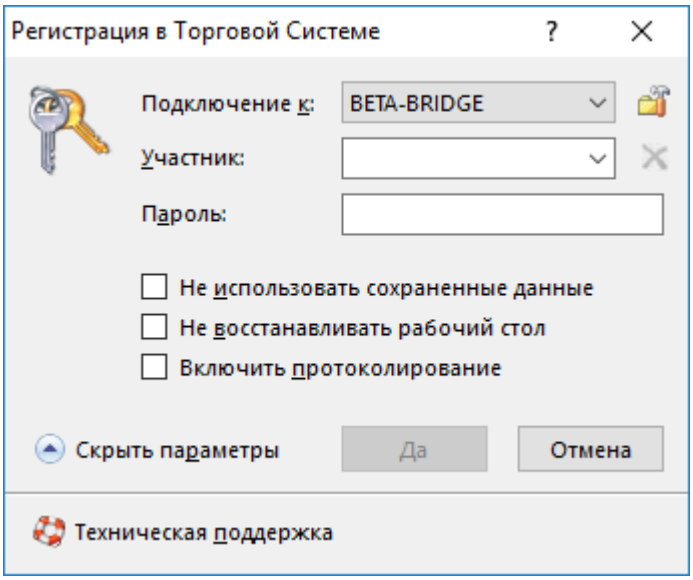




Загруженный сертификат должен отобразиться в разделе «Справочник сертификатов» \ «Локальный справочник» \ «Действующие сертификаты» в дереве сертификатов в левой части окна. Справочник настроен для работы с ТУМАР.

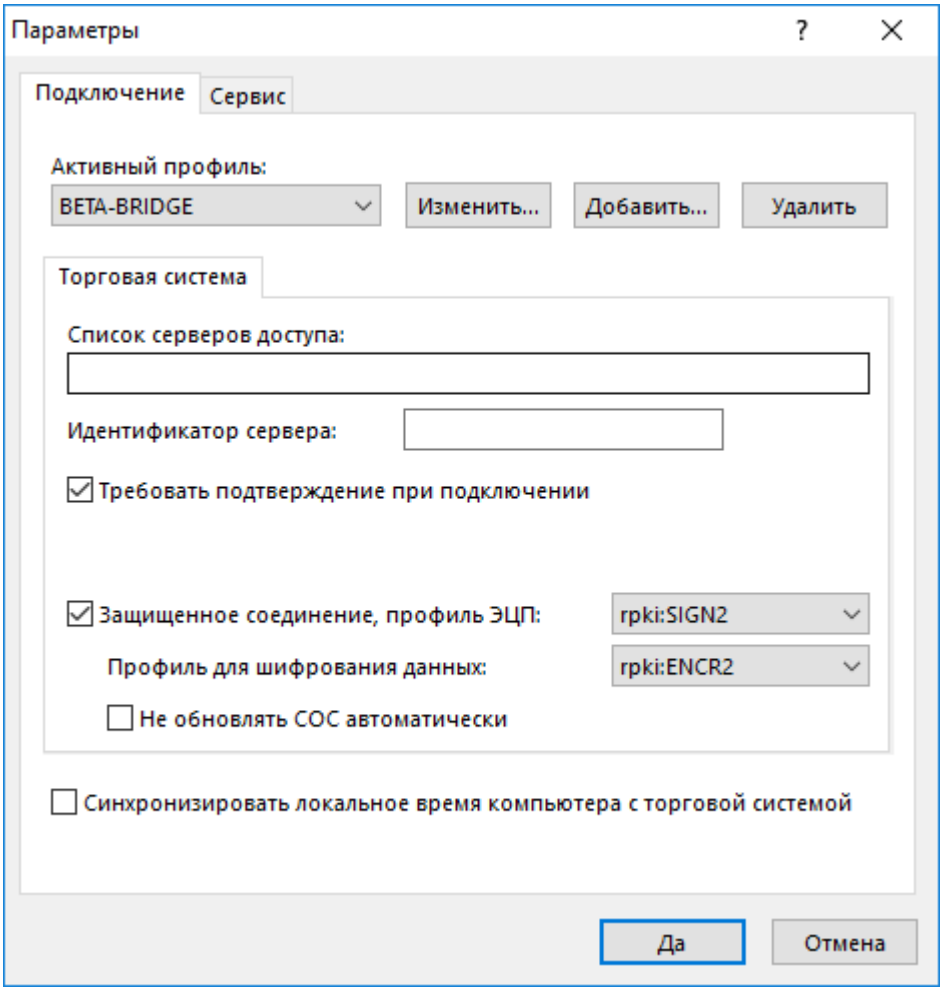
3. Настройка Trade SE (терминал торговой системы) на работу по ЭЦП.

Запустить терминал торговой системы Trade SE. В окне «Регистрация в Торговой Системе» выбрать раздел «Показать параметры» и перейти в режим настройки подключения.



Выбрать параметр «Защищеное соединение, профиль ЭЦП», и выбрать профили ранее создавшие в ПК «Справочник сертификатов».

Внимание: Настройки подключения «Список серверов доступа» и «Идентификатор сервера» выставить в соотвествии с инструкцией


Параметры
Подключение
Сервис
Активный профиль:
BETA-BRIDGE
Изменить...
Добавить...
Удалить
Торговая система
Список серверов доступа:
Идентификатор сервера:
Требовать подтверждение при подключении
Защищенное соединение, профиль ЭЦП:
rpki:SIGN2
Профиль для шифрования данных:
rpki:ENCR2
Не обновлять СОС автоматически
Синхронизировать локальное время компьютера с торговой системой
Да
Отмена