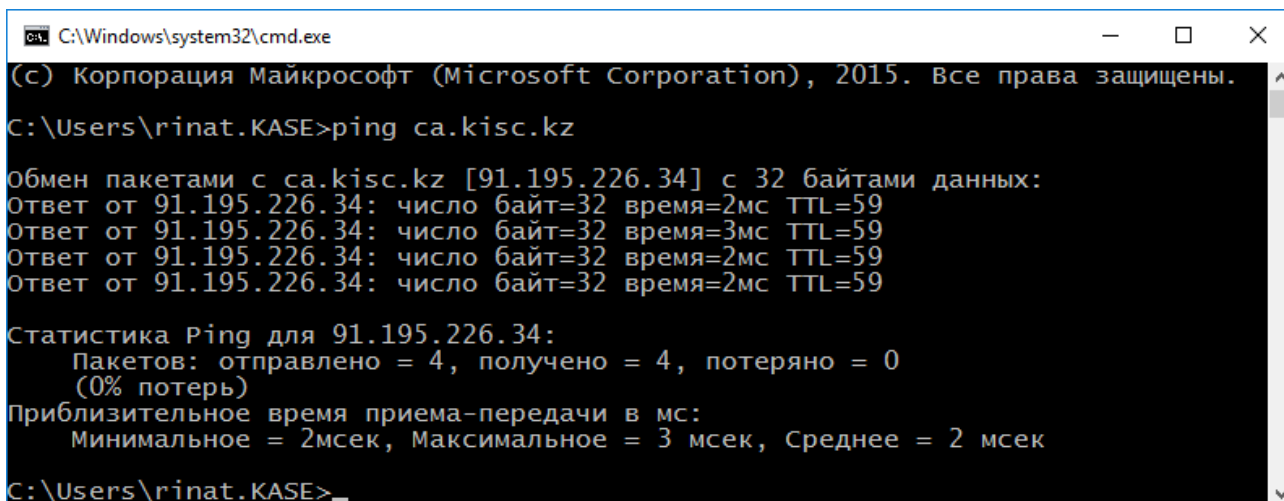


Руководство по настройке терминала торговой системы с использованием ЭЦП

ВАЖНО!

Для правильного функционирования Справочника сертификатов и Терминала TradeSE с использованием ЭЦП, необходимо открыть доступ к удостоверяющему центру ca.kisc.kz. Проверить можно следующим образом.

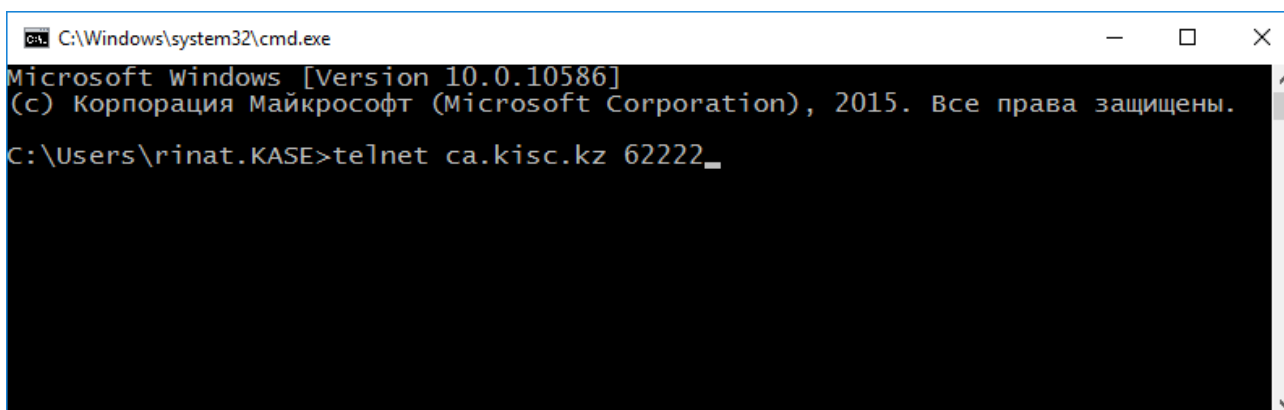


```
C:\Windows\system32\cmd.exe
(с) Корпорация Майкрософт (Microsoft Corporation), 2015. Все права защищены.
C:\Users\rinat.KASE>ping ca.kisc.kz

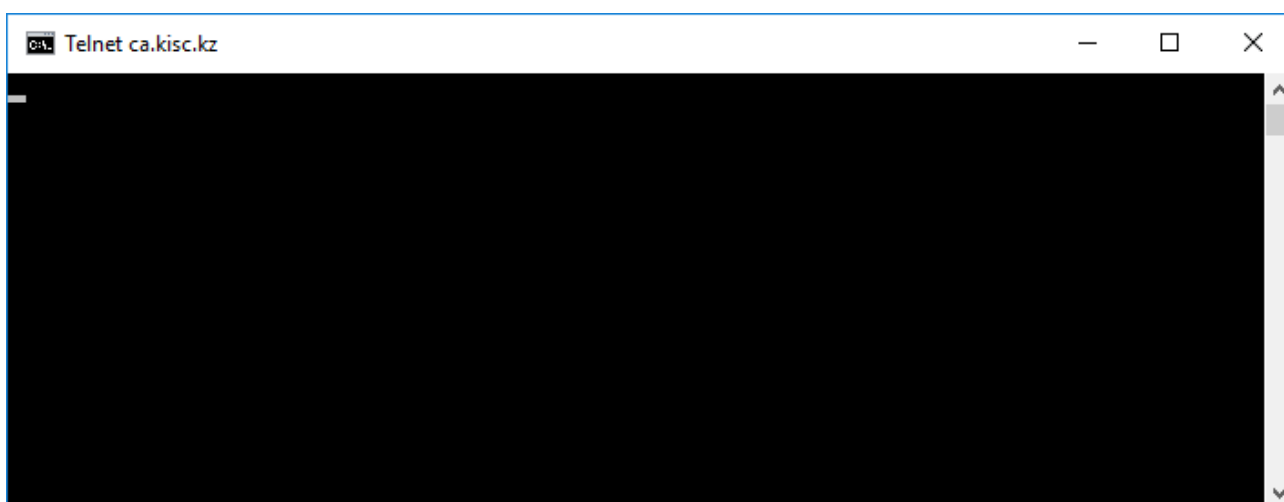
Обмен пакетами с ca.kisc.kz [91.195.226.34] с 32 байтами данных:
Ответ от 91.195.226.34: число байт=32 время=2мс TTL=59
Ответ от 91.195.226.34: число байт=32 время=3мс TTL=59
Ответ от 91.195.226.34: число байт=32 время=2мс TTL=59
Ответ от 91.195.226.34: число байт=32 время=2мс TTL=59

Статистика Ping для 91.195.226.34:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 3 мсек, Среднее = 2 мсек
C:\Users\rinat.KASE>
```

и



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(с) Корпорация Майкрософт (Microsoft Corporation), 2015. Все права защищены.
C:\Users\rinat.KASE>telnet ca.kisc.kz 62222_
```



```
Telnet ca.kisc.kz
```

В случае отсутствия доступа к удостоверяющему центру ca.kisc.kz, обратитесь к своим администраторам систем.

1. Установка ТУМАР-CSP

а) Скачать и установить последнюю версию криптодра ТУМАР-CSP по адресу:

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

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

Ключ подписи

The screenshot shows the 'Redacting profile' dialog box with the following settings:

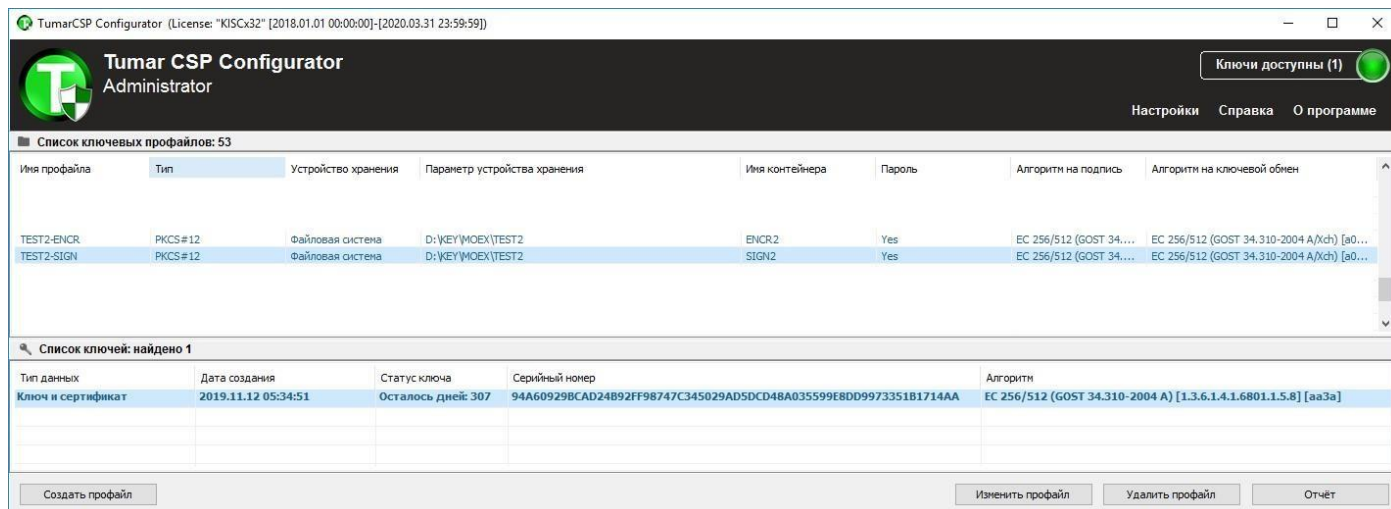
- Строка профайла: file://SIGN2:hex=822A2CDAC84B2D4F@/D:%5CKEY%5CMOEX%5CTEST2?salg=1.3.6.1.
- Имя профайла: TEST2-SIGN
- Устройство хранения: Файловая система
- Параметр устройства хранения: D:\KEY\MOEX\TEST2
- Пароль: [masked]
- Подтверждение: [masked]
- Формат ключевого контейнера: Tumar (.bin), Tumar (.pem), PKCS#12 (.pfx), PKCS#12 (.p12)
- Имя контейнера: SIGN2
- Алгоритм новых ключей для ключевого обмена: EC 256/512 (GOST 34.310-2004 A/Xch)
- Алгоритм новых ключей для подписи: EC 256/512 (GOST 34.310-2004 A)
- Buttons: Сохранить, Отмена

Ключ шифрования

The screenshot shows the 'Redacting profile' dialog box with the following settings:

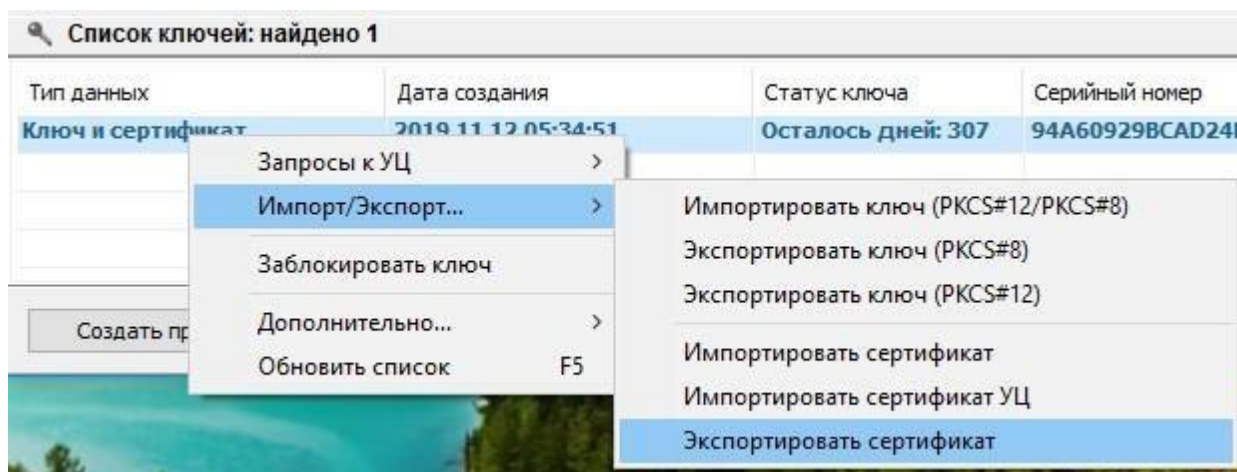
- Строка профайла: file://ENCR2:hex=101D3A63472E90A2@/D:%5CKEY%5CMOEX%5CTEST2?salg=1.3.6.1.
- Имя профайла: TEST2-ENCR
- Устройство хранения: Файловая система
- Параметр устройства хранения: D:\KEY\MOEX\TEST2
- Пароль: [masked]
- Подтверждение: [masked]
- Формат ключевого контейнера: Tumar (.bin), Tumar (.pem), PKCS#12 (.pfx), PKCS#12 (.p12)
- Имя контейнера: ENCR2
- Алгоритм новых ключей для ключевого обмена: EC 256/512 (GOST 34.310-2004 A/Xch)
- Алгоритм новых ключей для подписи: EC 256/512 (GOST 34.310-2004 A)
- Buttons: Сохранить, Отмена

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

- а) Создать временный пустой каталог с доступом на запись и чтение.
- б) 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 2а. Выполнить экспорт сертификата для ключа подписи и шифрования.



- в) 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:

<p>Корневое регистрационное свидетельство УЦ КЦМР. Алгоритм ГОСТ 34.310</p>	<p>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</p>	<p>Скачать в формате DER Скачать в формате PEM</p>	<p>Скачать список отозванных регистрационных свидетельств пользователей. Алгоритм ГОСТ 34.310</p>
---	---	---	---

Если описанный выше метод не работает воспользуйтесь следующим:


Скачать (с помощью браузера **Google Chrome** открыть в режиме инкогнито (**shift+ctrl+n**) или использовать другой браузер) корневой сертификат УЦ КЦМР (алгоритм ГОСТ 34.310) в формате DER и список отозванных сертификатов (алгоритм ГОСТ 34.310) по адресу:


<http://ca.kisc.kz/cgi/RevListGOST.crl>

https://www.kisc.kz/wp-content/uploads/2021/11/kisc_root_ca_gost.crt

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

В конечном итоге должно получиться как в примере:

 KISC_ROOT_CA_GOST.cer

 RevListGOST.crl

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

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

3. Установка ПК «Справочник сертификатов»

а) 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.

б) 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

Изменение профиля ✕

Имя профиля:

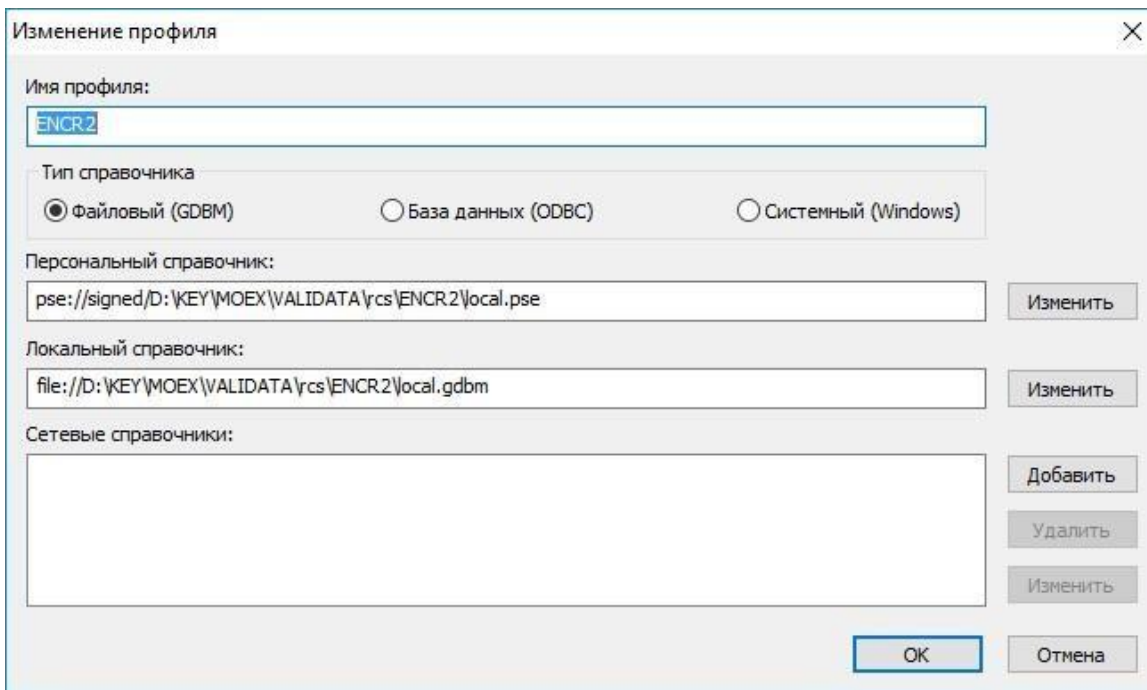
Тип справочника
 Файловый (GDBM) База данных (ODBC) Системный (Windows)

Персональный справочник:

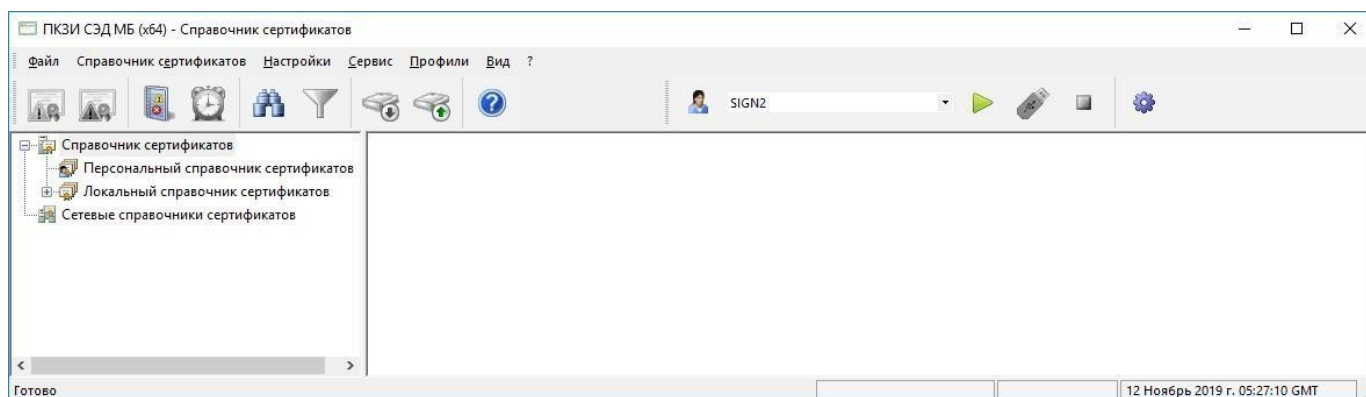
Локальный справочник:

Сетевые справочники:

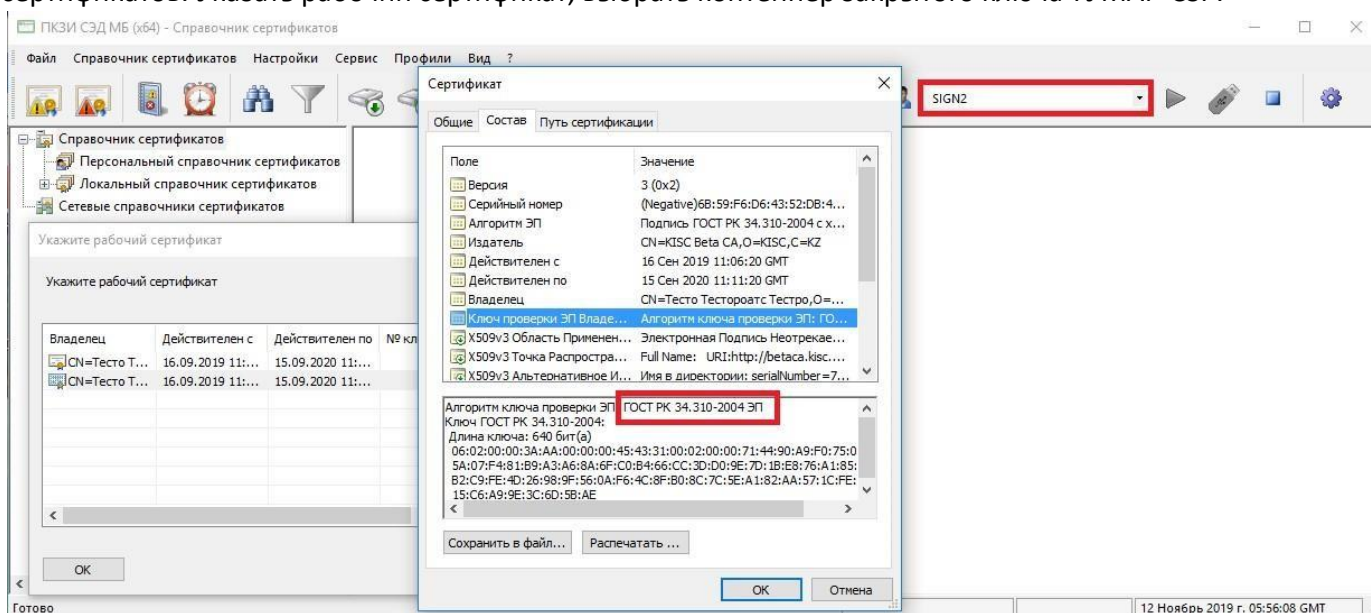
Профиль для сертификата шифрования

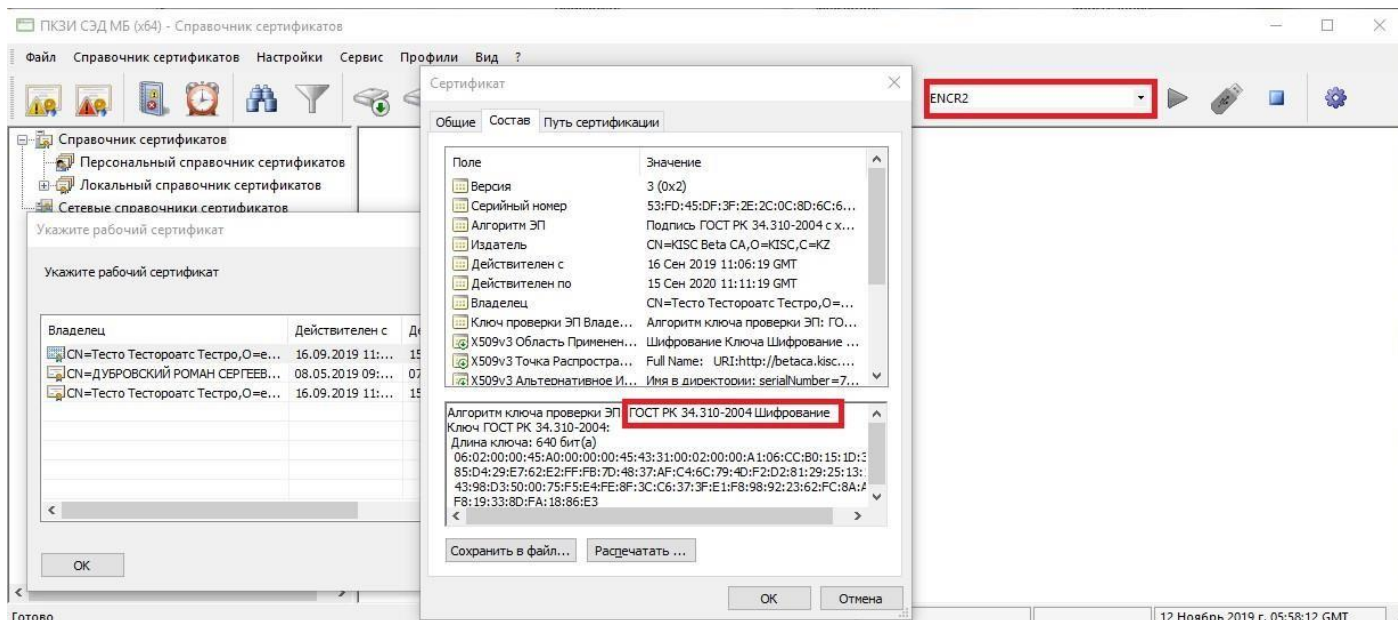


Выбрать созданный профиль в выпадающем списке профилей в панели инструментов и нажать кнопку «Загрузить профиль» (зеленый треугольник):



с) 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.

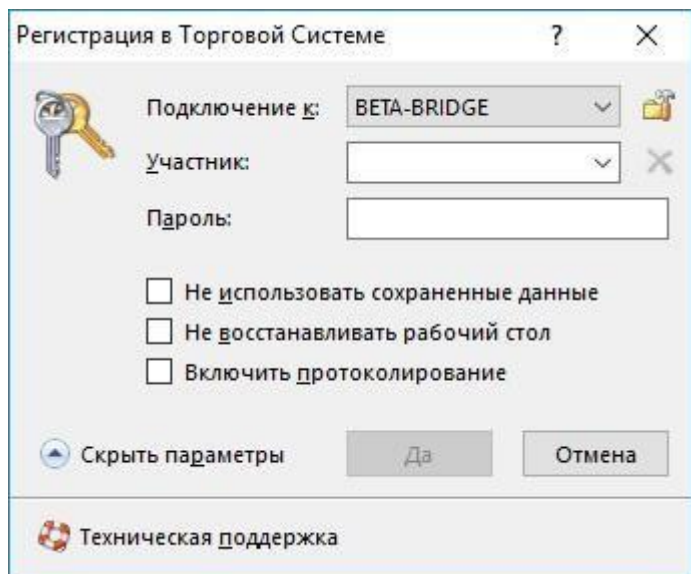




Загруженный сертификат должен отобразиться в разделе «Справочник сертификатов» \ «Локальный справочник» \ «Действующие сертификаты» в дереве сертификатов в левой части окна. Справочник настроен для работы с ТУМАР.

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

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

Параметры

Подключение **Сервис**

Активный профиль:
 BETA-BRIDGE

Торговая система

Список серверов доступа:

Идентификатор сервера:

Требуется подтверждение при подключении

Защищенное соединение, профиль ЭЦП:

Профиль для шифрования данных:

Не обновлять СОС автоматически

Синхронизировать локальное время компьютера с торговой системой

После выполнения операций по настройке терминала необходимо подать заявку на support@kase.kz с указанием записи поля Владелец. В теле заявки просим написать: Просим привязать данного Владельца ЭЦП к идентификатору участника (указать свой идентификатор).

Сертификат

Общие Состав Путь сертификации

Сертификат

X509v3 Альтернативное Имя Владельца:
 Имя в директории: serialNumber=120140015907/CN=АО Тест
 Имя в директории: serialNumber=821119301118/CN=Те Тест Тестор/L=Алматы/ST=Алматинская область

Владелец: UID=IIN821119301118 **CN=Те Тест Тестор,OU=АО Тест,O=TOO eTrade.kz,C=KZ**

Издатель: C=KZ,O=KISC,CN=KISC Root CA

Действителен с Действителен по

Ключ:
 Сертификат: 16 Янв 2020 09:15:06 GMT 15 Янв 2021 09:20:06 GMT