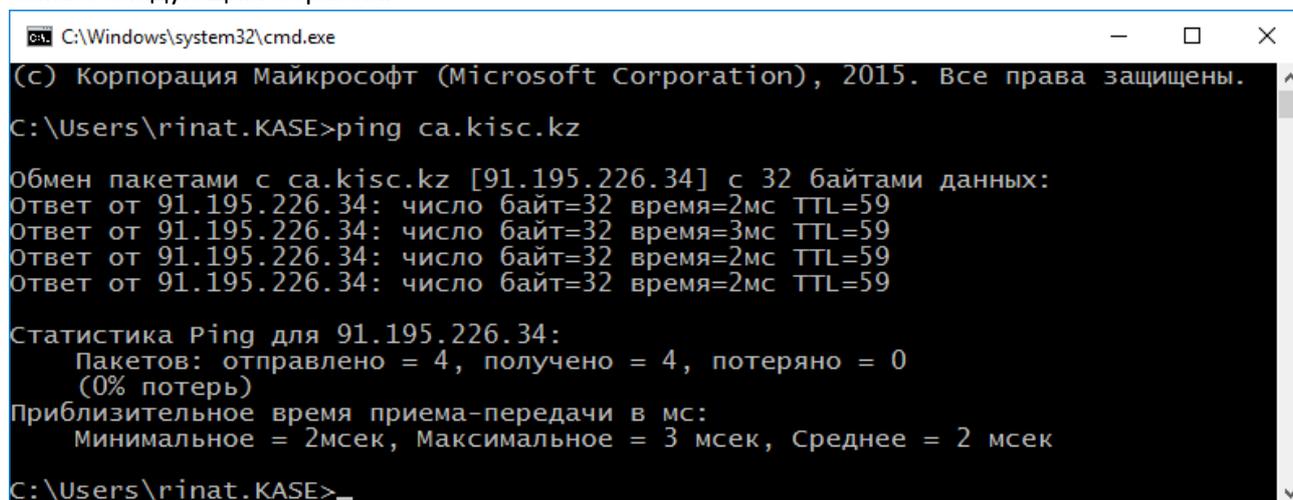


Руководство по настройке терминала торговой системы с использованием ЭЦП

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.

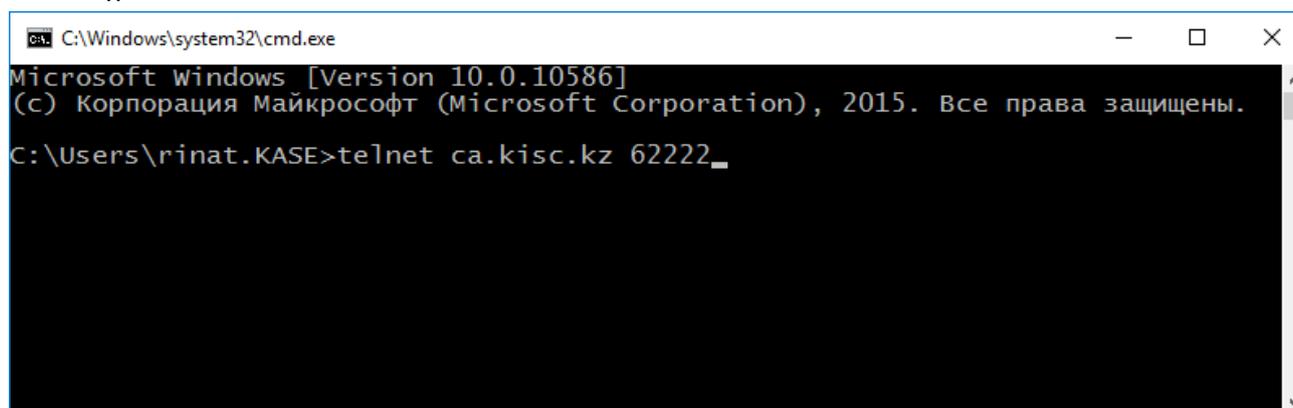


```
C:\Windows\system32\cmd.exe
(с) Корпорация Майкрософт (Microsoft Corporation), 2015. Все права защищены.
C:\Users\rinat.KASE>ping ca.kisc.kz

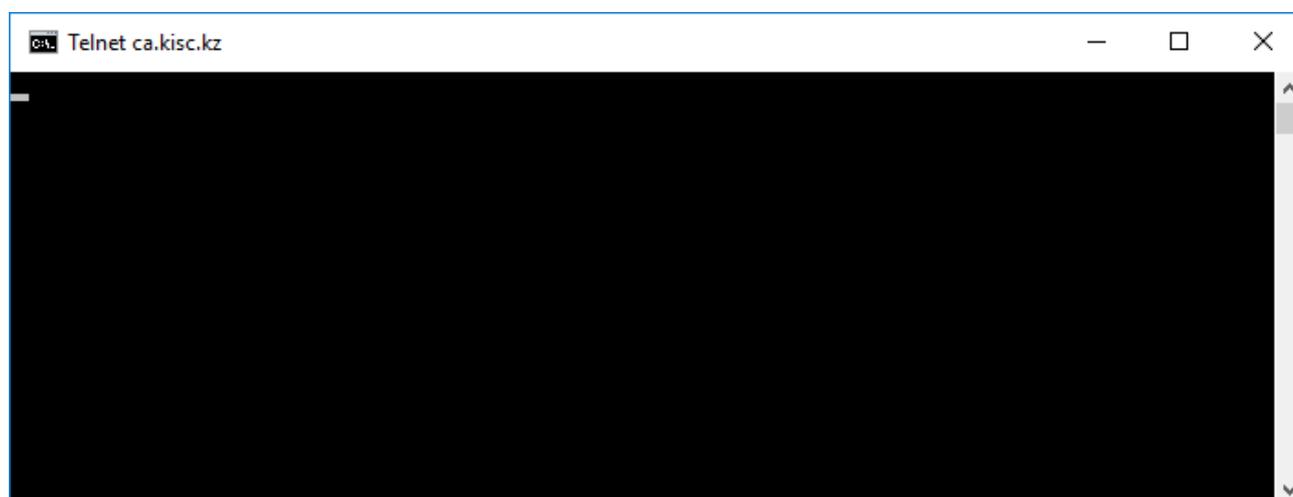
Обмен пакетами с ca.kisc.kz [91.195.226.34] с 32 байтами данных:
Ответ от 91.195.226.34: число байт=32 время=2мс TTL=59
Ответ от 91.195.226.34: число байт=32 время=3мс TTL=59
Ответ от 91.195.226.34: число байт=32 время=2мс TTL=59
Ответ от 91.195.226.34: число байт=32 время=2мс TTL=59

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) **Получение годовых ключей: Электронная подпись и Шифрования.**

1.1 Перейти на портал <https://ca.kisc.kz/auth>.

1.2 Открыть вкладку «Личный кабинет».

1.3 Нажать «Запрос на выпуск сертификата».

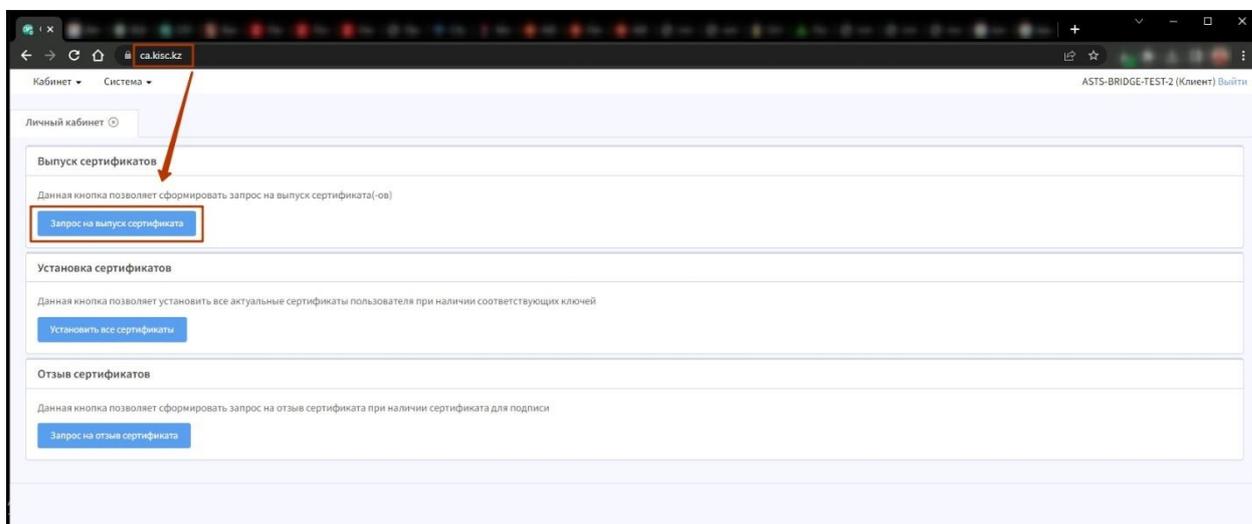


Рис. 1

2) **Выбираем следующие параметры:**

2.1 Выбор годового тарифа «KISC Certificate RK-02 (SIGN+EXCH)»

2.2 Устройство «Файловая система FSystem»

2.3 Сертификат для подписи - это временный ключ в утилите «TumarCSP Configurator».

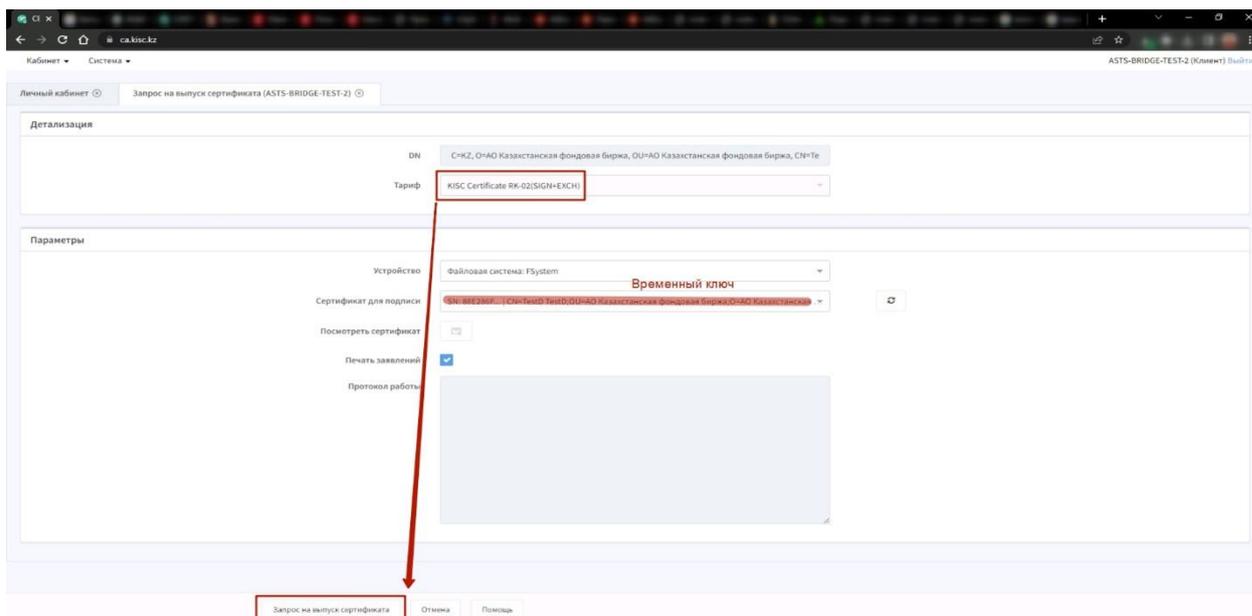


Рис. 2

3) Нажать на «Запрос на выпуск сертификата».

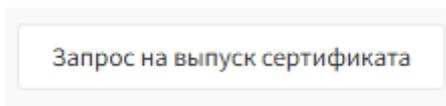


Рис. 3

4) Нажать «ОК».



Рис. 4

5) Годовые ключи должны появиться в «TumarCSP Configurator» в профайле «FSYSTEM»:

Тип ключа	Алгоритм
Шифрования	EC 256/512 (GOST 34.310-2004 A)[1.3.6.1.4.1.6801.1.5.8][aa3a]
Электронная подпись	EC 256/512 (GOST 34.310-2004 A/Xch) [1.3.6.1.4.16801.1.8.8][a045]

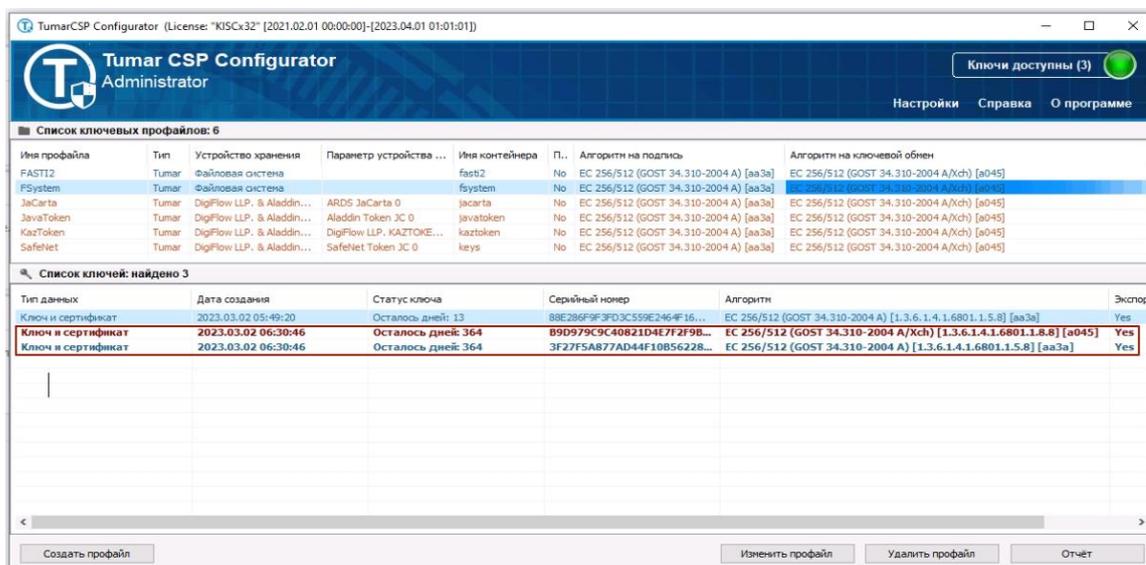


Рис. 5

6) Формирование каталога с годовыми ключами:

6.1 Создать временный пустой каталог с доступом на Запись и Чтение:

Этот компьютер > Локальный диск (C:) > key >

6.2 В контекстном меню окна «Список ключей» утилиты “TumarCSP Configurator” выбрать команду «Импорт/Экспорт...»

6.3 Нажать “Экспортировать ключ (PKCS#12)” и сохранить ключ в каталог, созданный на шаге 6.1

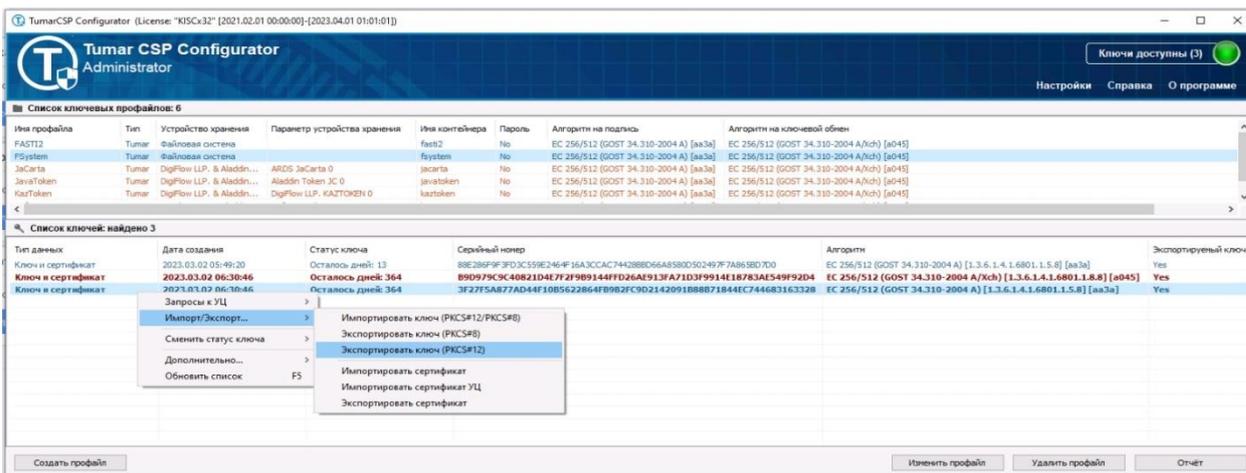


Рис. 6 – Ключ Электронная подпись

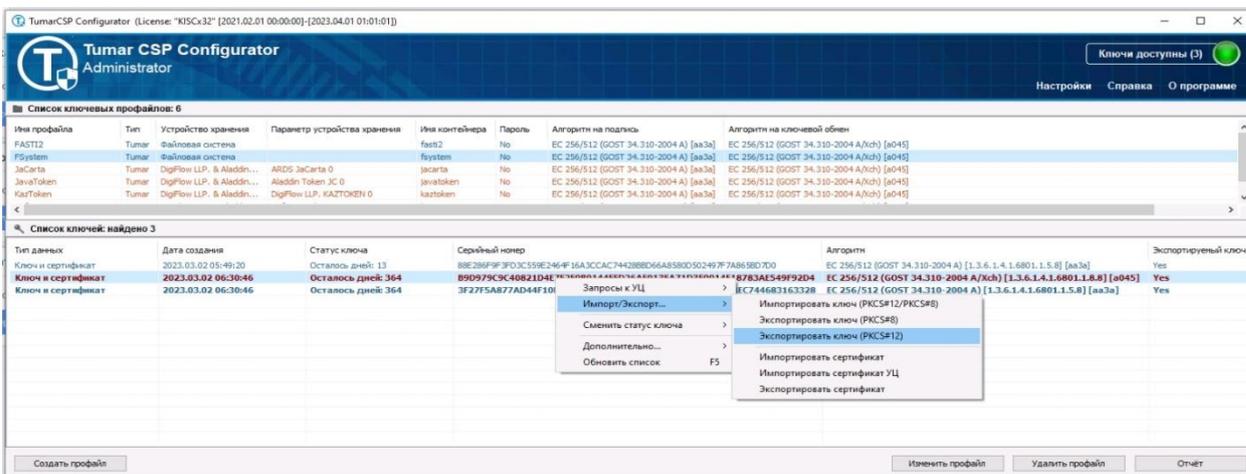


Рис. 7 – Ключ Шифрования

7) Заведение ключевых профайлов в утилите “TumarCSP Configurator”:

7.1 Создать ключевые профайлы для годовых ключей.

7.2 Загрузить в профайл «SIGN» ключ Электронная подпись Рис. 8.

Редактирование профайла

Строка профайла
file://SING@/C:%5CKEY?salg=1.3.6.1.4.1.6801.1.5.8&ext=px

Параметры профайла
Имя профайла: SING
Устройство хранения: Файловая система
Параметр устройства хранения: C:\KEY Обзор

Пароль: _____ Подтверждение: _____

Формат ключевого контейнера:
 Tumar (.bin) Tumar (.pem) PKCS#12 (.pfx) PKCS#12 (.p12)

Имя контейнера: SING

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)

Сохранить Отмена

Рис. 8

7.3 Загрузить в профайл «ENCR» ключ Шифрования Рис. 8.

Редактирование профайла

Строка профайла
file://ENCR@/C:%5CKEY?salg=1.3.6.1.4.1.6801.1.5.8&ext=px

Параметры профайла
Имя профайла: ENCR
Устройство хранения: Файловая система
Параметр устройства хранения: C:\KEY Обзор

Пароль: _____ Подтверждение: _____

Формат ключевого контейнера:
 Tumar (.bin) Tumar (.pem) PKCS#12 (.pfx) PKCS#12 (.p12)

Имя контейнера: ENCR

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)

Сохранить Отмена

Рис. 9

8) Экспорт сертификаты(DER)(* .cer)

8.1 Выбрать ключ (**SIGN**) в утилите “TumarCSP Configurator” > В контекстном меню выбрать команду «Импорт/Экспорт...» > “Экспортировать сертификат» и сохранить сертификат в кодировке (DER)(* .cer) Рис. 10 в каталог на шаге 6.1

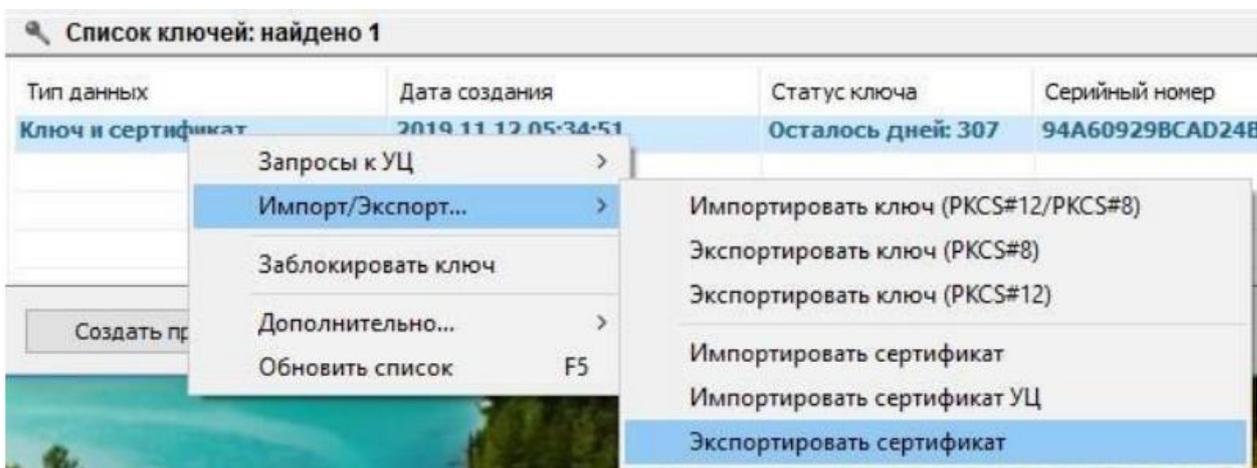


Рис. 10

8.2 Выбрать ключ (**ENCR**) в утилите “TumarCSP Configurator” > В контекстном меню выбрать команду «Импорт/Экспорт...» > “Экспортировать сертификат» и сохранить сертификат в кодировке (DER)(* .cer) Рис. 9 в каталог на шаге 6.1

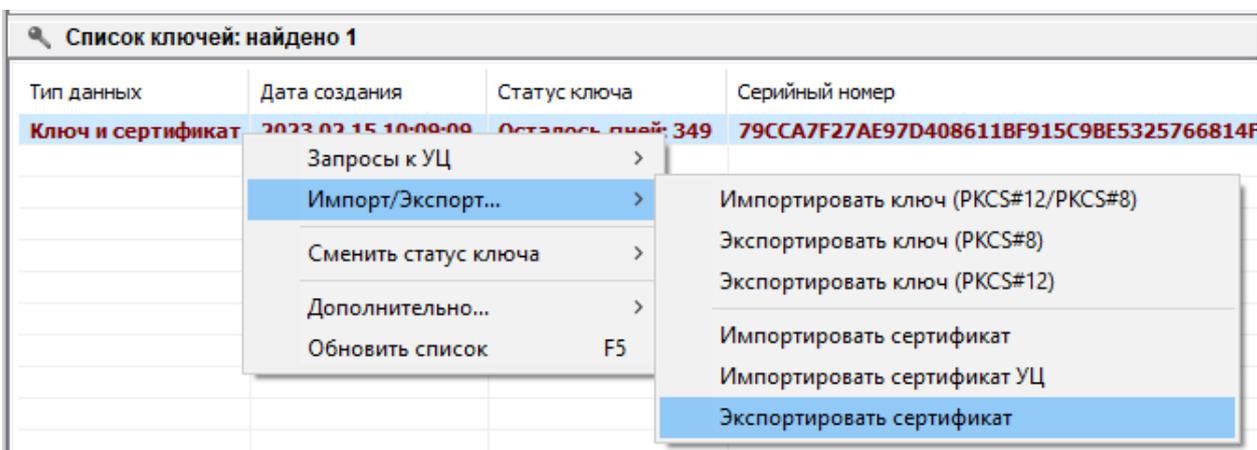


Рис. 11

9) **Скачать** (⚠ При загрузке через **Google Chrome** могут возникнуть проблемы, поэтому рекомендуется использовать браузер **Mozilla Firefox**) корневой сертификат УЦ КЦМР (алгоритм ГОСТ 34.310) в формате DER и список отозванных сертификатов (алгоритм ГОСТ 34.310) на портале npck.kz Рис. 12

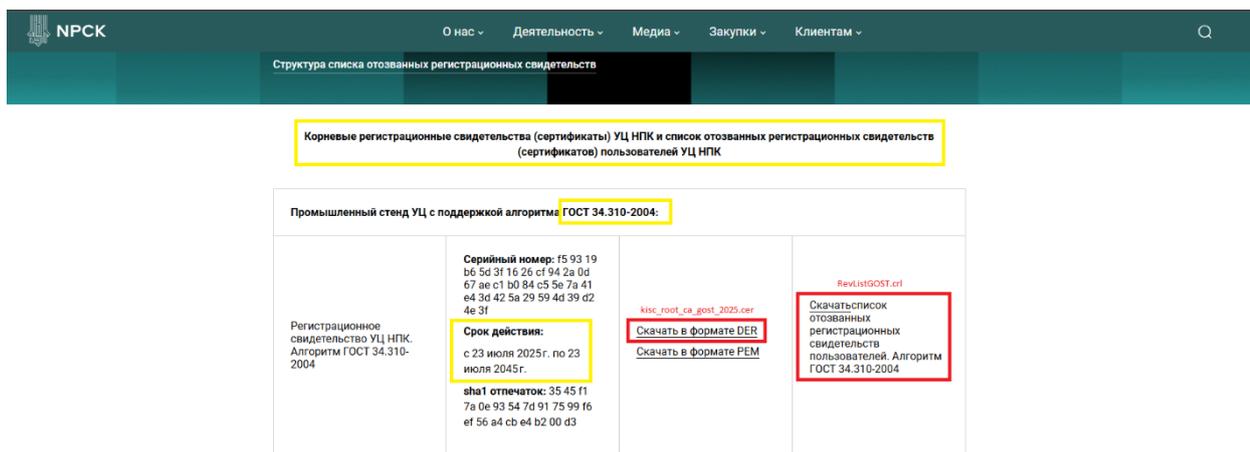


Рис. 12

Или можно скачать по ссылкам:

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

9.2 https://npck.kz/wp-content/uploads/2025/08/kisc_root_ca_gost_2025_der.zip

9.3 В конечном итоге должно получиться Рис. 13.

 kisc_root_ca_gost_2025.cer	12.09.2025 16:02	Сертификат	1 КБ
 RevListGOST.crl	12.09.2025 16:02	Список отозванных сертификатов	296 КБ

Рис. 13

9.4 Сохранить в каталог на шаге 6.1

10) Установка ПК «Справочник сертификатов»:

10.1 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

10.1 Запустить «Справочник сертификатов»

10.2 Создать два профиля, выбрав команду «Профили»

10.3 «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 Рис. 14-15.

Изменение профиля

Имя профиля:
SIGN2

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

Персональный справочник:
pse://signed/D:\KEY\MOEX\VALIDATA\rcs\SIGN2\local.pse Изменить

Локальный справочник:
file://D:\KEY\MOEX\VALIDATA\rcs\SIGN2\local.gdbm Изменить

Сетевые справочники:
Добавить
Удалить
Изменить

OK Отмена

Рис. 14 - Профиль **Электронная подпись**

Изменение профиля

Имя профиля:
ENCR2

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

Персональный справочник:
pse://signed/D:\KEY\MOEX\VALIDATA\rcs\ENCR2\local.pse Изменить

Локальный справочник:
file://D:\KEY\MOEX\VALIDATA\rcs\ENCR2\local.gdbm Изменить

Сетевые справочники:
Добавить
Удалить
Изменить

OK Отмена

Рис. 15 - Профиль **Шифрования**

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

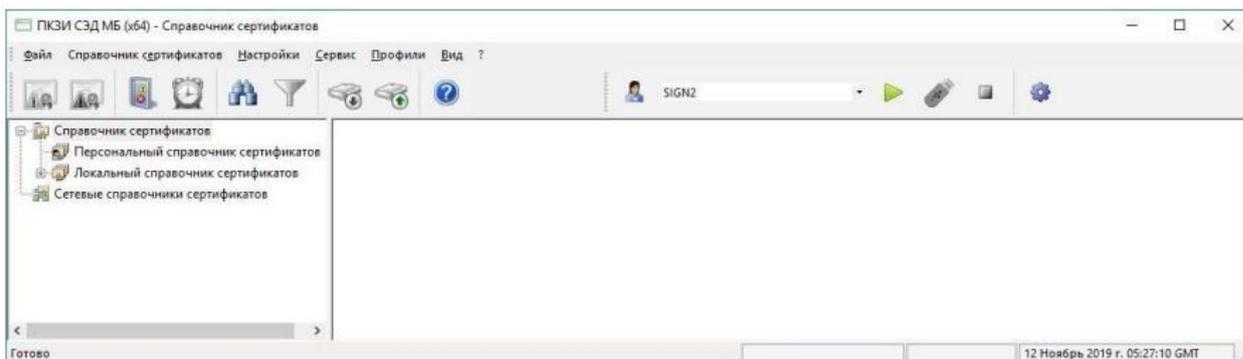


Рис. 16

10.5 Выбрать команду «Сервис» > «Сформировать справочник из каталога», указать каталог, в который на шаге 6.1 были сохранены собственный сертификат, сертификат УЦ КЦМР и список отозванных сертификатов. Указать рабочий сертификат, выбрать контейнер закрытого ключа в утилите “TumarCSP Configurator”.

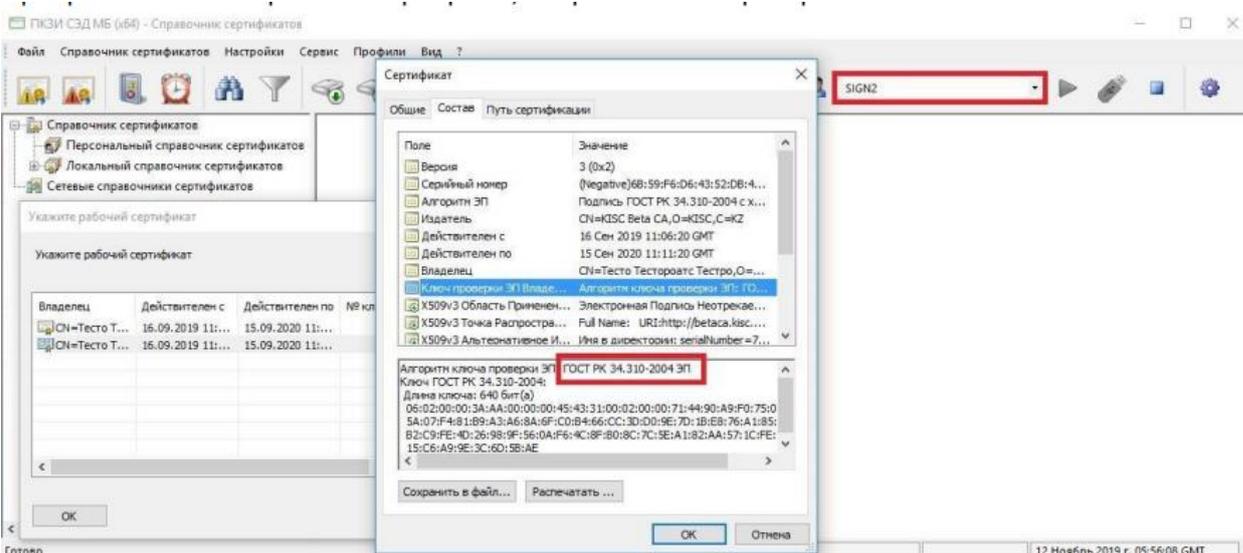


Рис. 17

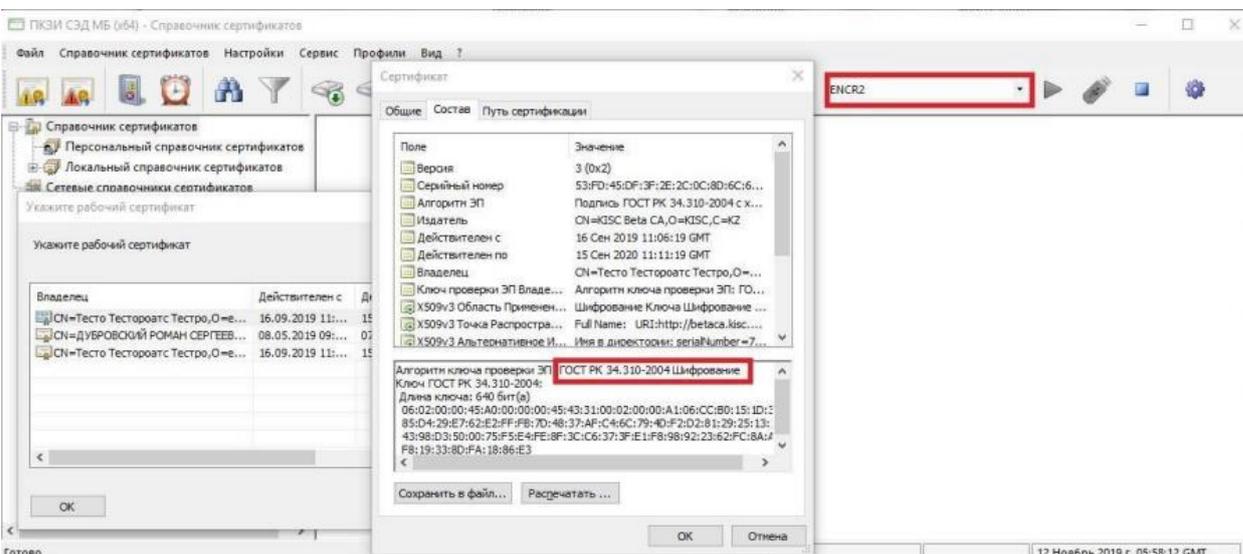


Рис. 18

10.5 Загруженный сертификат должен отображаться в разделе «Справочник сертификатов» \ «Локальный справочник» \ «Действующие сертификаты» в дереве сертификатов в левой части окна. Справочник настроен для работы с “TumarCSP Configurator”.

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

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

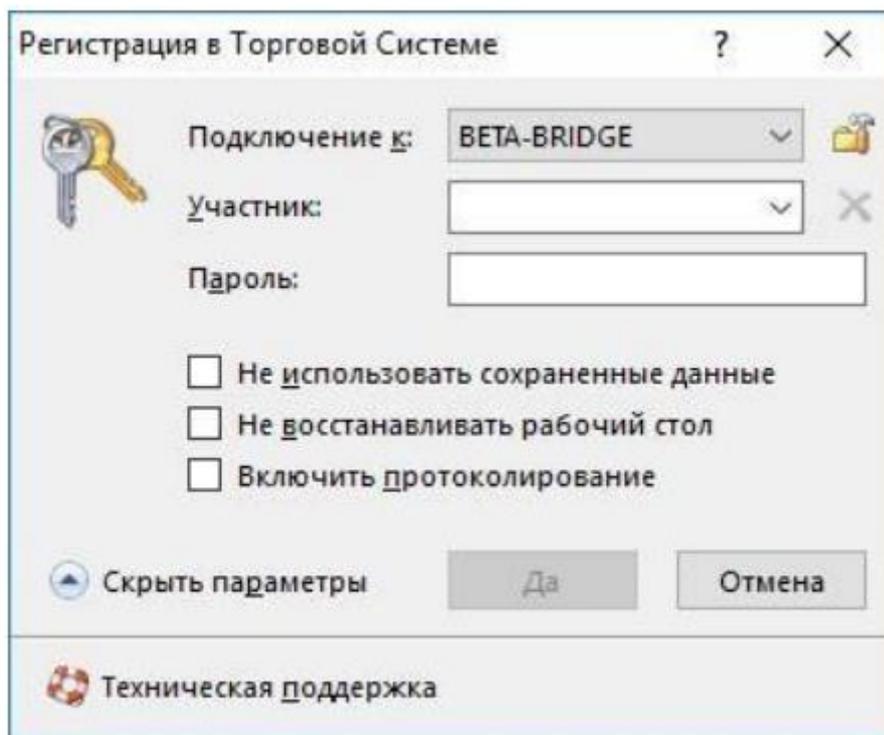


Рис. 19

11.2 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

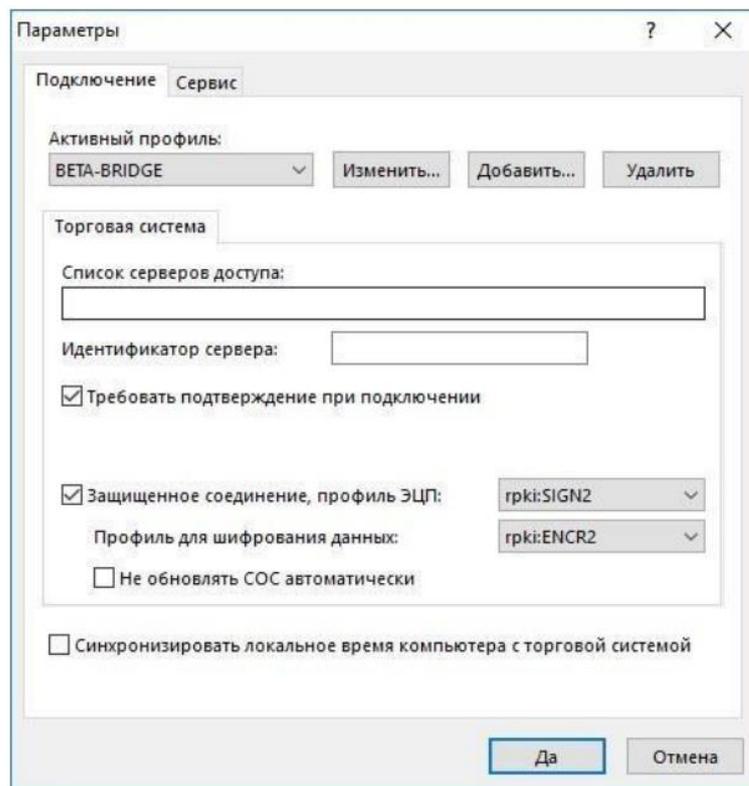


Рис. 20

11.3 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) Рис. 21

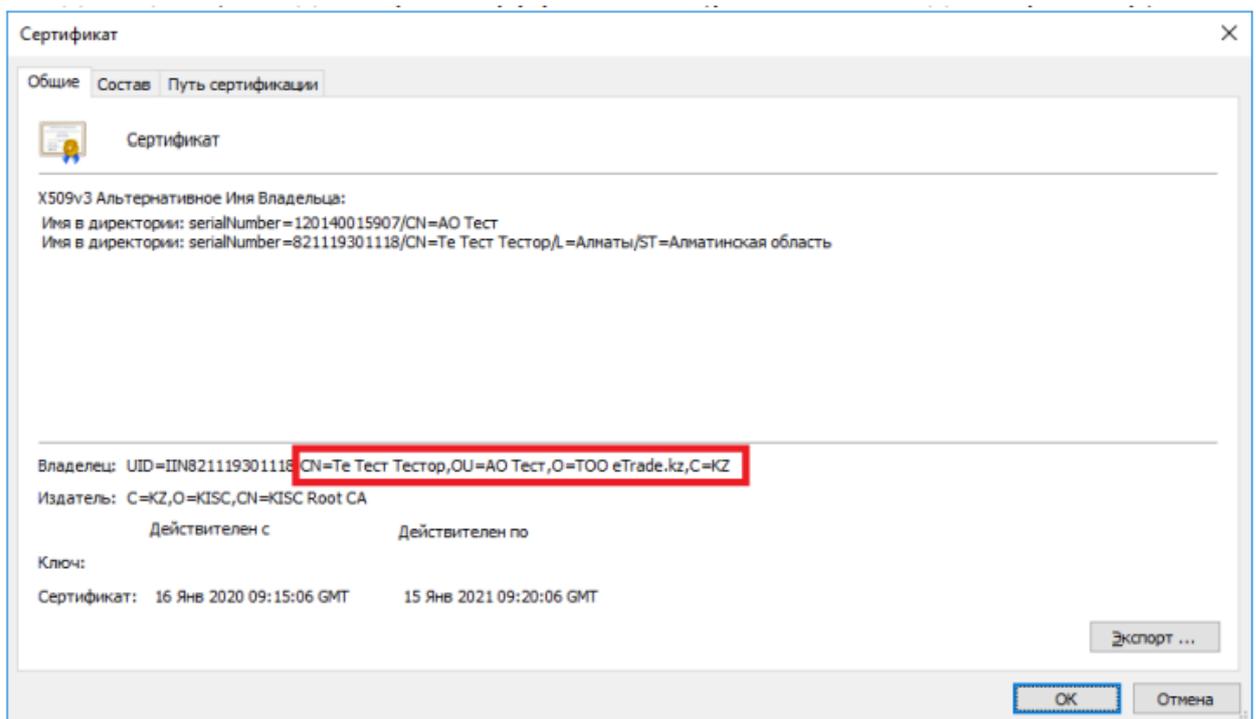


Рис. 21