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.







👞 Telnet ca.kisc.kz	—	×
		^
		~

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

1. Установка ТУМАР-СSP

а) 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

дактирование профаи	іла		
Строка профайла			
file://SIGN2:hex=822A2	2CDAC84B2D4F@	P/D:%5CKEY%5CMOEX%5	CTEST2?salg=1.3.6.1.
Параметры профайла			
Имя профайла:	TEST2-SIGN		-
Устройство хранения:	Файловая сис	тема	~
Параметр устройства х	ранения:		
D: KEY MOEX TEST2			∨ Обзор
Пароль:		Подтверждение:	
•••••		•••••	
Формат ключевого конт	гейнера:		
O Tumar (.bin)	^r umar (.pem)	PKCS#12 (.pfx)	OPKCS#12 (.p12)
Имя контейнера:	SIGN2		
Алгоритм новых ключе	й для ключево	о обмена:	
Алгоритм новых ключе EC 256/512 (GOST 34.3	й для ключево 10-2004 A/Xch)	о обмена:	~
Алгоритм новых ключе EC 256/512 (GOST 34.3 Алгоритм новых ключе	й для ключевоі 10-2004 A/Xch) й для подписи:	го обмена:	~
Алгоритм новых ключе EC 256/512 (GOST 34.3 Алгоритм новых ключе EC 256/512 (GOST 34.3	ій для ключевої 10-2004 A/Xch) ій для подписи: 10-2004 A)	го обмена:	~
Алгоритм новых ключе EC 256/512 (GOST 34, 3 Алгоритм новых ключе EC 256/512 (GOST 34, 3	ий для ключево 10-2004 A/Xch) ий для подписи: 10-2004 A)	го обмена:	~

Ключ шифрования

Строка профайла				
file://ENCR2:hex=101D3	3A63472E90A2@	P/D:%5CKEY%5CMOEX%5	CTEST2?	alg=1.3.6.1.
Параметры профайла				
Имя профайла:	TEST2-ENCR			
Устройство хранения:	Файловая сис	тема		~
Параметр устройства хр	оанения:			
D: KEY MOEX \TEST2			~	Обзор
Пароль:		Подтверждение:		
		•••••		
Формат ключевого конт	ейнера:			
 ○ Tumar (.bin) ○ Т Имя контейнера: 	umar (.pem)	PKCS#12 (.pfx)	Орк	CS#12 (.p12
 ○ Tumar (.bin) ○ Т Имя контейнера: Алгоритм новых ключе 	umar (.pem) ENCR2 й для ключевог		Орк	CS#12 (.p12
○ Tumar (.bin) ○ Т Имя контейнера: Алгоритм новых ключе ЕС 256/512 (GOST 34.3	umar (.pem) ENCR2 й для ключевог 10-2004 A/Xch)	• РКСЅ#12 (.pfx) то обмена:	Орк	CS#12 (.p12
 ☐ Tumar (.bin) ☐ Т Имя контейнера: Алгоритм новых ключе ЕС 256/512 (GOST 34.3 Алгоритм новых ключе 	umar (.pem) ENCR2 й для ключевог 10-2004 A/Xch) й для подписи:	• РКСЅ#12 (.pfx) го обмена:	Орк	CS#12 (.p12
 О Tumar (.bin) О Т Имя контейнера: Алгоритм новых ключе ЕС 256/512 (GOST 34.3 Алгоритм новых ключе ЕС 256/512 (GOST 34.3 	umar (.pem) ENCR2 й для ключевог 10-2004 A/Xch) й для подписи: 10-2004 A)	• РКСЅ#12 (.pfx) то обмена:	Орк	CS#12 (.p12
 Титаг (.bin) Т Имя контейнера: Алгоритм новых ключе ЕС 256/512 (GOST 34.3 Алгоритм новых ключе ЕС 256/512 (GOST 34.3 	umar (.pem) ENCR2 й для ключевог 10-2004 A/Xch) й для подписи: 10-2004 A)	• РКСЅ#12 (.pfx) го обмена:	Орк	CS#12 (.p12

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

TumarCSP Configu	irator (License: "KISCx3	32" [2018.01.01 00:00:00]-[202	0.03.31 23:59:59])					- 0	×
Adn	nar CSP Cor ninistrator	nfigurator					н	Ключи доступны (1) астройки Справка Опрогра	амме
П Список ключевы	х профайлов: 53								
Имя профайла	Тип	Устройство хранения	Параметр устр	ийства хранения	Имя контейнера	Пароль	Алгоритм на подпись	Алгоритм на ключевой обмен	^
TEST2-ENCR	PKCS#12	Файловая система	D:\KEY\MOEX\T	ST2	ENCR2	Yes	EC 256/512 (GOST 34	EC 256/512 (GOST 34.310-2004 A/Xch) [a	a0
1E512-5IGN	PRCS#12	Фаиловая Система	D: WEY MOEX (I	512	STONZ	res	EC 256/512 (GUS1 34	EC 256/512 (GUST 34.310-2004 A/XCR) [8	30
🔍 Список ключей: і	найдено 1								×
Тип данных	Дата созда	ания Ста	гус ключа	Серийный номер			Алгоритм		
Ключ и сертификат	2019.11.1	2 05:34:51 Ост	алось дней: 307	94A60929BCAD24B92FF98	747C345029AD5DCD48A035599E8DI	09973351B1714AA	EC 256/512 (GOST 34.310-20	04 A) [1.3.6.1.4.1.6801.1.5.8] [aa3a]	
Создать профайл							Изменить профайл Уда	алить профайл Отчёт	

2. Формирование каталога с сертификатами

а) 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 2а. Выполнить экспорт сертификата для ключа подписи и шифрования.

Тип данных	Дата со	Дата создания Статус ключ		Серийный номер	
Ключ и сертифии	at 2019 1	1 12 05-34-51	1 Осталось дней: 307 94А60929ВС		
	Запросы к уц Импорт/Экспорт	> V	Импортировать ключ (РКС		
Cosearь or	Заблокировать клю Дополнительно	ч ^з З	Экспортировать ключ (PKCS#8) Экспортировать ключ (PKCS#12) Импортировать сертификат Импортировать сертификат УЦ		
Cosdano ne	Обновить список	F5 V			
		3	Экспортировать сертификат		

<u>И</u> мя файла:	
<u>Т</u> ип файла:	Сертификаты(DER)(*.cer)
 Скрыть папки 	Сохранить Отмена

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	<u>Скачать в</u> формате <u>DER</u> <u>Скачать в</u> формате <u>PEM</u>	<u>Скачать список отозванных регистрационных свидетельств пользователей. Алгоритм ГОСТ 34.310</u>
		Скачать в	

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»

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

<u>http://kase.kz/ru/kase_moex_connection/</u> 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

		×
○База данных (ODBC)	○ Системный (Windows)	
IDATA\rcs\SIGN2\ocal.pse		Изменить
rcs\SIGN2\local.gdbm		Изменить
		Добавить
		Удалить
		Изменить
	OK	Отмена
	○ База данных (ODBC) IDATA\rcs\SIGN2\Jocal.pse rcs\SIGN2\Jocal.gdbm	ОБаза данных (ODBC) ОСистемный (Windows) IDATA\rcs\SIGN2\Jocal.pse rcs\SIGN2\Jocal.gdbm

Профиль для сертификата шифрования

1зменение про <mark>ф</mark> иля			3
Имя профиля:			
ENCR2			
Тип справочника			
• Файловый (GDBM)	ОБаза данных (ODBC)	○ Системный (Windows)	
Персональный справочник:			
pse://signed/D:\KEY\MOEX\VAL	IDATA\rcs\ENCR2\local.pse		Изменить
Локальный справочник:			
file://D:\KEY\MOEX\VALIDATA\	rcs\ENCR2\local.gdbm		Изменить
Сетевые справочники:			
			Добавить
			Удалить
-		1	Изменить
		ОК	Отмена

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

🛅 ПКЗИ СЭД МБ (x64) - Справочник сертификатов			- 🗆 X
<u>Ф</u> айл Справочник с <u>е</u> ртификатов <u>Н</u> астройки <u>С</u> ервис <u>П</u> рофили <u>В</u> ид ?			
🖬 🖬 🗓 🕅 🍸 😪 🌏	SIGN2	• 🕨 🖉 💷 🚳	•
Справочник сертификатов Персональный справочник сертификатов Локальный справочник сертификатов Сетевые справочники сертификатов			
Готово		12 H	Ноябрь 2019 г. 05:27:10 GMT

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-СSP.

🛅 ПКЗИ СЭД МБ (x64) - Справочник сертификатов		- 🗆 ×
Файл Справочник сертификатов Настройки Сервис Профи	ли Вид ?	
🙀 🙀 🖲 💆 🧥 🍸 🍕 🤇	сертификат × sign2	• 🕨 🖉 🕼
Справочник сертификатов Персональный справочник сертификатов Локальный справочник сертификатов Сетевые справочник сертификатов Укажите рабочий сертификат Укажите рабочий сертификат	Общие Состав Путь сертификации Поле Значение • Версия 3 (0x2) • Серийный номер (Negative)68:59:F6:D6:43:52:D8:4 Общие Серийный номер (Negative)68:59:F6:D6:43:52:D8:4 Издатель CN=KISC Deta CA,O=KISC,C=KZ • Действителен с 16 Ceн 2019 11:06:20 GMT • Действителен по 15 Ceн 2020 11:11:20 GMT • Паладелец CN=Tecro Tecropoarc Tecrpo,0= •	
Владелец Действителен с Действителен по № кл □ (N=Tecro T 16.09.2019 11: 15.09.2020 11: □ (CN=Tecro T 16.09.2019 11: 15.09.2020 11: ⊂ СК	Сохранить в файл Распечатать	

Овайл Справочных сертификатов Пастройки Сертификатов Справочных сертификатов Соравочных сертификатов Сертификатов Сертификатов Персональный справочных сертификатов Поле Значение Сертификатов Ухажите рабочий сертификатов Поле Значение Сертификатов Ухажите рабочий сертификатов Поле Значение Поле Значение Ухажите рабочий сертификатов Поле Значение Поле Значение Поле Значение Поле Значение Поле Значение Поле Значение Поле Значение Поле Значение Укажите рабочий сертификатов Поле Овлаконсо ПСК 23.310-2004 Ск Поле Поле Значение (Констесто Тесторо, Оче 16.09.2019 11 Поле 15 Сен 2019 11.1019 ОИТ ОК Поле 15 Сен 2019 11.0	🛅 ПКЗИ СЭД МБ (x64) - Справочник сертифи	икатов				— E	X
Общие Состав Путь сертификации Обще Сост	Файл Справочник сертификатов Настрой	йки Сервис Про	фили Вид ? Сертификат		× ENCR2		<u></u>
Впаделец Действителен с Ди Ключ проверки ЭП Владе Алгорити ключа Шифрование ключа Шифрование к Ключ проверки ЭП владе Ключ проверки ЭП: ГО Ключ проверки ЭП ГОСТ РК 34.310-2004!! Алгорити ключа проверки ЭП ГОСТ РК 34.310-2004!! Ключ проверки ЭП ГОСТ РК 34.310-2004!! Ключ проверки ЭП ГОСТ РК 34.310-2004!! Алгорити ключа проверки ЭП ГОСТ РК 34.310-2010:!! Ключ Посой 45: А0:00:00:45: 43:31:00:02:00:01:45: 43:31:00:02:00:01:41:05: CC:80:15: 10: 12: Ключ Посой 45: А0:00:00:01:45: 43: 31:00:02:20:00:01:45: 43: 31:00:02:20:00:01:45: 43: 31:00:02:00:00:01:45: 43: 31:00:02:00:00:01:45: 43: 31:00:02:00:00:01:45: 43: 31:00:02:00:00:01:45: 43: 31:00:02:00:00:01:45: 43: 40: 00:00:00:00:45: 43: 31:00:02:00:00:01:45: 43: 31:00:02:00:00:00:01:45: 43: 31:00:02:00:00:00:00:00:00:00:00:00:00:00:	Справочник сертификатов Персональный справочник сертифи Персональный справочник сертификат Сетевые справочники сертификат Укажите рабочий сертификат Укажите рабочий сертификат	икатов	Общие Состав Путь сертифика Поле Версия Серийный номер Алгорити ЭП Издатель Действителен с Владелец	Ции 3 (0x2) 53:F0:45:DF:3F:2E:2C:0C:8D Подпись ГОСТ РК 34.310-200 С0=KISC Beta CA,0=KISC,C- 16 Сен 2019 11:06:19 GMT 15 Сен 2020 11:11:19 GMT CN=Tect Decroport Tectoro	6C:6 4c x kZ		
OK Othena	Владелец Ди СN=Тесто Тестороатс Тестро,О=е 16 СN=ДУБРОВСКИЙ РОМАН СЕРГЕЕВ 08 СП-Тесто Тестороатс Тестро,О=е 16 СМ СМ	ействителен с Д. 6.09.2019 11 15 8.05.2019 09: 07 6.09.2019 11 15	Ключ проверки ЭП Владе ЗХ09v3 Область Применен ХХ09v3 Область Применен ХХ09v3 Альтернативное И ХХ09v3 Альтернативное И ХХ09v3 Альтернативное И Алгорити ключа проверки ЭП Г Ключ ГОСТ РК 34.310-2004: Длина ключа: 640 биг (rd) Об:02:00:00:45:A0:00:00:00:05: SS:D4:29:47:62:22:FF:F8:70:48: 43:96:03:55:00:07:5F:SE:47:E1:87: Сохранить в файл Распеча	Алгоритн ключа проверки Э Шифрование Ключа Шифор Full Name: URI:http://betaca Иня в дисектооии: serialNum OCT PK 34.310-2004 Шифрован 43:31:00:02:00:00:A1:06:CCB 37:AF:C4:6C:79:4D:F2:D2:81:2 3C:C6:37:3F:E1:F8:98:92:23:6 атать	1: ГО ание kisc уе = v уг. 15: ID:: 9:25: 13: : F:: C:SA:: >)		

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.

егистра	ция в Торговой Сис	теме	?	×
3	Подключение <u>к</u> :	BETA-BRIDGE	5E ~	
	<u>У</u> частник:		~	>
	Пароль:			
	Не <u>в</u> осстанавл Включить <u>п</u> ро	ивать рабочий этоколирование	стол	
		Ла	Отмен	
CK	лыть па <u>р</u> аметры		2.233.227	ia

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

		~ 1/	Ізменить	Добавить	Удалить
Торговая <mark>си</mark> с	тема				
Список сере	зеров дост	упа:			1
Идентифика	атор серве	pa:			
🗹 Требоват	ть подтвер	ждение при	1 подключен	нии	
		19793577 - 1974).	مسه عالله	rpki:SIGN2	~
🗹 Защищен	ное соеди	нение, про	филь Эцн.		
🗹 Защищен Профил	ное соеди ъ для шиф	інение, про рования да	филь Эцп. нных:	rpki:ENCR2	~
⊠ Защищен Профил ☐ Не об	ное соеди ь для шиф Sновлять С	інение, про рования да :ОС автомат	филь Эцп. нных: :ически	rpki:ENCR2	~

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).

Сертифика	т			×
Общие Со	остав Путь сертификации			
	Сертификат			
Х509v3 Ал Имя в дир Имя в дир	пьтернативное Имя Владельца: ректории: serialNumber=1201400159 ректории: serialNumber=8211193011	07/CN=AO Тест 18/CN=Te Tecт Tecтop/L=Алматы/ST=A	лматинская область	
Владелец	: UID=IIN821119301118 CN=Te Tec	r Тестор,OU=AO Тест,O=TOO eTrade.k	z,C=KZ	
Издатель	: C=KZ,O=KISC,CN=KISC Root CA			
	Действителен с	Действителен по		
Ключ:				
Сертифик	кат: 16 Янв 2020 09:15:06 GMT	15 Янв 2021 09:20:06 GMT		
				<u>Э</u> кспорт
				ОК Отмена