

Инструкция по созданию ключа электронной подписи (ЭП).

Системные требования:

- Windows 7 и выше.
- Для Google Chrome, Mozilla Firefox, Яндекс необходимо установить дополнительно расширения https://brokerkf.ru/doc/manuals/browsers_settings.pdf.
- Браузер Internet Explorer 11 (не EDGE!) https://old.brokerkf.ru/doc/uc/How-to-runIE_win10_11.pdf
- Для MacOS необходимо использовать продукты виртуализации, такие как Parallels Desktop VMware Fusion, Virtual box, и др.

При возникновении технических проблем просьба сделать снимок экрана, описать ситуацию и прислать по адресу uc@brokerkf.ru, указав номер договора о брокерском обслуживании.

Процедура создания ключа ЭП состоит из:

[Шаг 1. Настройка браузера](#)

[Шаг 2. Генерация ключа. Запрос на выпуск сертификата ключа проверки ЭП](#)

[Шаг 3. Подписание документов](#)

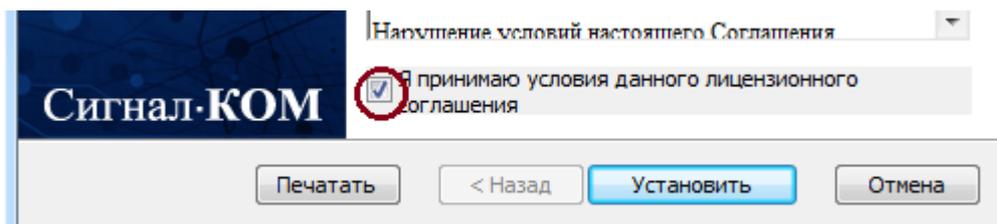
[Шаг 4. Создание резервной копии – необходимый этап в процессе генерации ключа](#)

Шаг 1. Настройка браузера

Запустите браузер, пройдите по ссылке <https://webca.brokerkf.ru/>, скачайте и установите плагин:

* Для корректной работы Вам необходимо **скачать и установить плагин**

- [Физическое лицо](#)
- [Юридическое лицо](#)



→ Готово

Шаг 2. Генерация ключа. Запрос на выпуск сертификата ключа проверки ЭП.

Перед началом генерации Вам необходимо создать папку (например, **ключ202X**) на флэшке или локальном диске. **НЕЛЬЗЯ** создавать папку на диске С или рабочем столе.

Выберите необходимый пункт:

- [Физическое лицо](#)
- [Юридическое лицо](#)

В появившемся окне **“Формирование запроса на сертификат”** заполните форму.

Если Вы авторизовались в Личном кабинете, данные заполнятся автоматически, необходимо проверить правильность заполнения.

[Вверх](#)

ФОРМИРОВАНИЕ ЗАПРОСА НА СЕРТИФИКАТ

Для генерации криптографических ключей и формирования запроса на сертификат заполните поля формы.

Поля, помеченные *, обязательны к заполнению.

* Номер договора:	<input type="text" value="номер ДБО"/>
* Ф.И.О. владельца ключа:	<input type="text" value="ФИО полностью"/>
* Адрес электронной почты:	<input type="text" value="your@e-mail.ru"/>
* Страна (CountryName):	<input type="text" value="RU"/>
* Город:	<input type="text" value="город"/>
<input type="button" value="Заполнить по сертификату"/> <input type="button" value="Очистить"/>	
* Каталог ключевого носителя:	<input type="text" value="файловая система"/> <input type="text" value="L:\ключ2022"/> <input type="button" value="Обзор..."/>
<input checked="" type="checkbox"/> Включить защиту ключевого контейнера паролем	
<input type="checkbox"/> Подписать запрос	
<input type="button" value="Сформировать запрос"/>	

Возможно заполнить форму автоматически (Заполнить по сертификату), указав путь к ранее выпущенному сертификату (файл с расширением .cer в папке cert).

Поля, отмеченные звездочкой (*), обязательны для заполнения

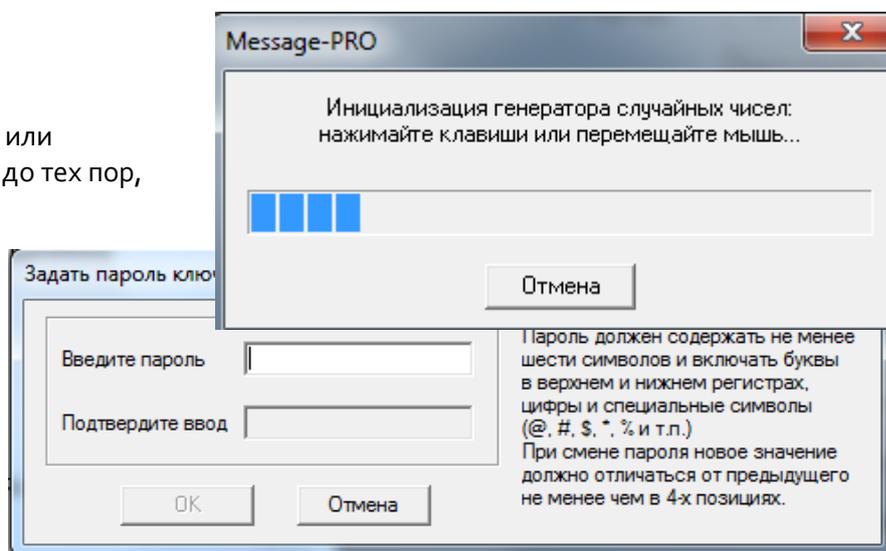
- Номер договора на брокерское обслуживание
- Ф.И.О. владельца ключа - **фамилия, имя и отчество полностью** на русском языке.
- Адрес электронной почты - **авторизованный** e-mail.
- Для юридических лиц: наименование организации и должность владельца сертификата.
- Каталог ключевого носителя - укажите папку **«ключ2022»**, где будет храниться Ваш новый секретный ключ.
Запомните указанный Вами путь.

Нажмите кнопку **«Сформировать запрос»**

Система предложит ввести пароль для секретного ключа. Придумайте пароль и введите его в форму. Пароль должен состоять не менее, чем из шести знаков. Обратите внимание на раскладку (РУС/ENG), Caps Lock.

Не забывайте пароль - впоследствии он будет использоваться при подключении к QUIK и для подписи поручений в Личном кабинете.

Двигайте мышью в пределах этого окна или нажимайте любые клавиши клавиатуры до тех пор, пока шкала не заполнится полностью:



При появлении печатной формы запроса нажмите кнопку

Продолжить

Распечатывать НЕ нужно.

-----END CERTIFICATE REQUEST-----

1.3. Область действия сертификата ключа проверки ЭП (сведения об отношениях, при осуществлении которых электронные документы с электронной подписью, сформированной при помощи соответствующих ключей электронной подписи, будут иметь юридическое значение) и Организатора подсистемы СЭД (в случае наличия):
ЭДО КИТ Финанс (АО)

Настоящим, ФИО полностью
(фамилия, имя, отчество владельца сертификата ключа проверки ЭП)
соглашается с обработкой своих персональных данных Компанией и/или Организатором подсистемы СЭД и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых он является, относятся к общедоступным персональным данным.

Участник СЭД

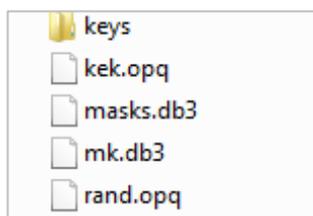
(владелец сертификата ключа проверки ЭП)

_____/_____/_____
(Фамилия И.О.)

Продолжить

Появление окна, содержащего **регистрационный номер запроса**, означает, что Ваш запрос на сертификацию ключа получен Удостоверяющим Центром.

Убедитесь, что на указанном Вами носителе появились необходимые файлы *ключевого контейнера*:



Созданный ключ ЭП должен храниться только у Вас. Никогда не передавайте Ваш ключевой носитель третьим лицам.

Шаг 3. Подписание документов.

В течение трёх рабочих дней Вы получите на авторизованный адрес электронной почты печатную форму Сертификата ключа проверки ЭП в формате PDF.

Документ необходимо подписать и передать в Компанию доступным Вам способом:

- персонально, посетив офис Компании
- почтовым отправлением в адрес Компании (191119, Россия, город Санкт-Петербург, улица Марата, дом 69-71)

Следуйте инструкциям, полученным от Удостоверяющего Центра на Ваш электронный адрес. В случае возникновения дополнительных вопросов или затруднений обратитесь за консультацией к сотрудникам Удостоверяющего Центра компании КИТ Финанс Брокер.

Шаг 4. Создание резервной копии – необходимый этап в процессе генерации ключа

В случае выхода из строя съёмного носителя с ключами ЭП, заражении компьютерными вирусами, случайном удалении файлов ключа ЭП, Вы сможете продолжить работу, используя запасную копию, для этого Вам необходимо просто скопировать папку «КИТ Финанс новые ключи» с файлами на отдельный носитель.

В Компании копии Вашего ключа ЭП нет и в случае проблем, процедуру генерации необходимо будет проводить заново.

Хранить ключевой носитель с резервной копией необходимо в условиях, исключающих доступ к нему третьих лиц.

Соблюдайте правила безопасности при работе с ключевым носителем:

- Не передавайте носитель с ключами ЭП третьим лицам
- Не оставляйте носитель с ключами ЭП в открытом доступе (например, на столе) при отсутствии на рабочем месте
- Извлекайте носитель с ключами ЭП из компьютера каждый раз после завершения его использования
- Не оставляйте носитель с ключами ЭП установленным в компьютер при неактивности