ООО «КИБЕРПЛАТ»

Россия, 123610, г. Москва, ЦМТ-2,
Краснопресненская наб., д.12, подъезд №7
Телефон: 8 (495) 967-02-20 Факс: 8 (495) 967-02-08
http://www.cyberplat.ru Email: info@cyberplat.ru

CyberPlat

Russia, 123610, Moscow, WTC-2,
Krasnopresnenskaya nab., 12, Entrance #7
Phone: +7 (495) 967-02-20 Fax: +7 (495) 967-02-08
http://www.cyberplat.com Email: info@cyberplat.com

Создание ключа подписанта системы CyberFT с помощью программы GenKey

Руководство пользователя

2019

Аннотация

В настоящем документе описан процесс создания комплекта ключей подписанта, необходимых для документооборота в рамках системы CyberFT. Разработка ООО «КИБЕРПЛАТ».

Версии документа

Версия документа	Дата	Изменения	Исполнители
1.0	13.08.2018	Начало отсчета версий документа.	Асеева В.А., Бондарь А.А., Максимов П.А.
1.1	11.02.2019	Обновлены разделы: 2 Создание ключа на токене и 3 Подготовка Акта о признании электронной подписи. Добавлен раздел 2.3 Пример настроек при создании ключей на токене.	Асеева В.А., Бондарь А.А., Максимов П.А.

Содержание

1 Скачивание программы GenKey

Для работы в системе электронного документооборота сети CyberFT необходимо создать ключи электронной подписи для подписантов документов.

Для создания ключей скачайте с сайта программу генерации ключей GenKey.

Дистрибутив программы можно скачать по данному адресу

http://download.cyberft.ru/GenKey/GenKey.zip.

Распакуйте архив в папку C:\...\ GenKey .

Ключи для работы в системе CyberFT могут создаваться на токене, а также в файле на жестком диске компьютера или флеш-носителе. **Хранение ключей на токене более надежно**.

Настоящая инструкция содержит порядок работы при создании ключей с помощью программы GenKey, а также при формировании акта о признании электронной подписи. Подробности работы с программой GenKey вы можете прочитать в Руководстве пользователя «Генерация ключей с помощью программы GenKey».

Внимание! Ключи необходимо выпускать для лиц, обладающих полномочиями подписантов.

2 Создание ключей

2.1 Создание ключей на токене

В настоящем разделе описано создание ключей криптосистемы RSA **на токене** с помощью программы генерации ключей GenKey**.** Правила работы с программой описаны в руководстве пользователя «Генерация ключей с помощью программы GenKey»

Особенности создания ключей **в файле** описаны в разделе «Создание ключей в файле». Файлы могут размещаться на жестком диске компьютера или на USB флеш-носителе.

Ключи необходимо выпускать для лиц, обладающих **полномочиями подписантов**.

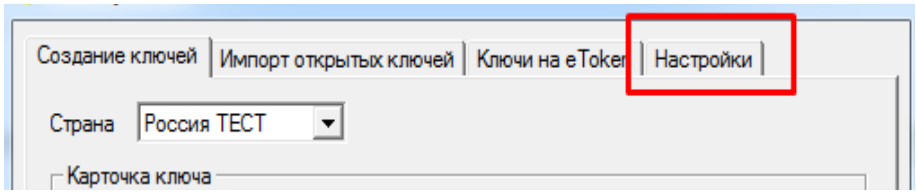
Внимание!

- Хранение ключей на токене более надежно, чем хранение ключей в файле.
- Разрешенные типы токенов описаны в руководстве пользователя программы GenKey .
- Перед тем, как создавать ключи на токене, внимательно прочитайте прилагаемую к токену **документацию и установите драйверы**, поставляемые в комплекте с токеном.
- Процедуры **начальной инициализации** и **установки пароля токена** производятся клиентом самостоятельно при помощи поставляемых с устройством программ.

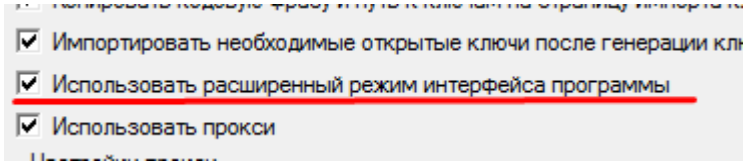
Порядок действий

1. При создании ключей на токене до запуска программы GenKey **подключите токен** к компьютеру через USB-порт.
2. Запустите программу создания ключей **Genkey.exe**.
3. Перейдите на вкладку ***Настройки***.

   Обратите внимание, что вкладка ***Ключи на eToken*** будет отображаться на экране, если на вашем компьютере установлен драйвер токена.

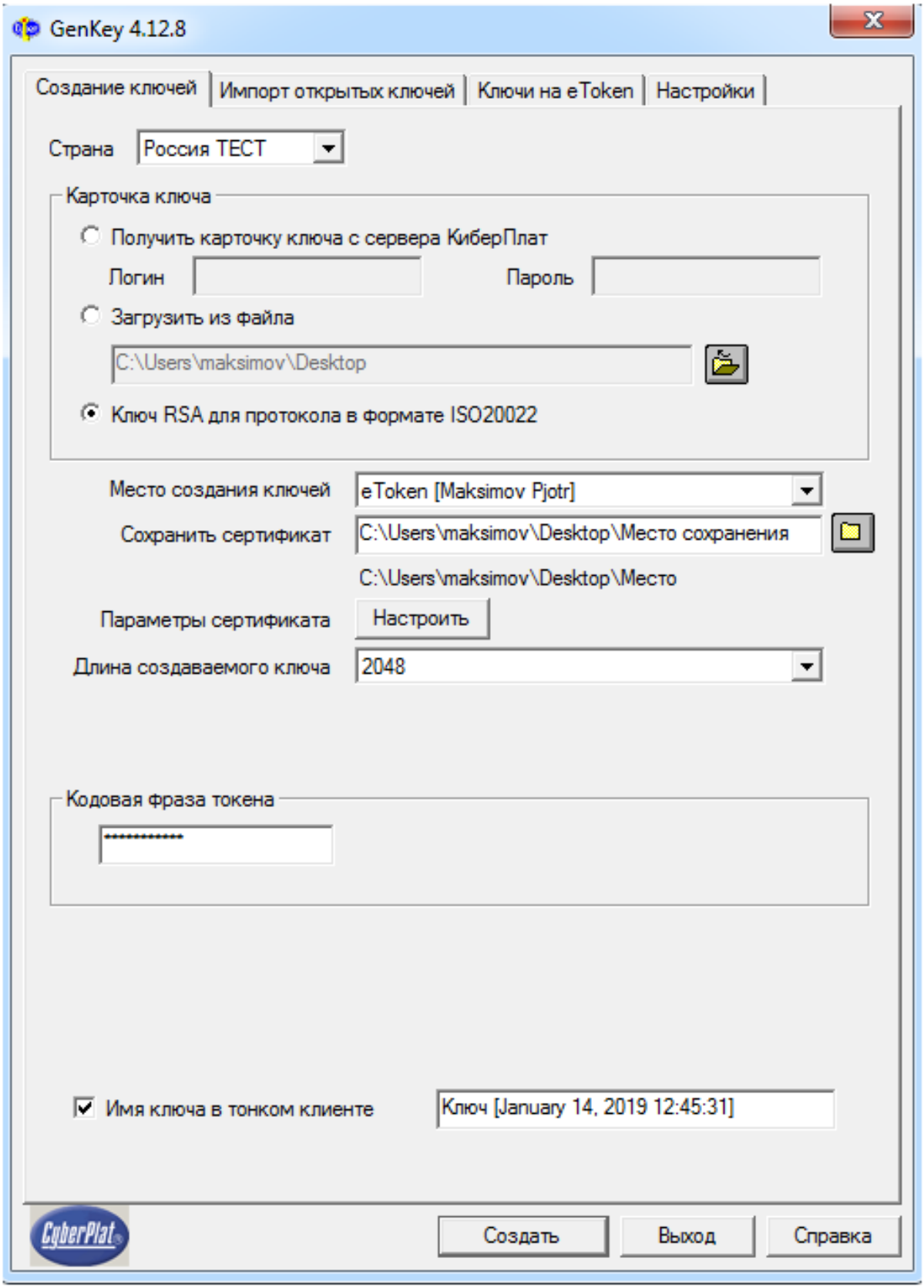


4. Установите отметку ***Использовать расширенный режим интерфейса программы.***

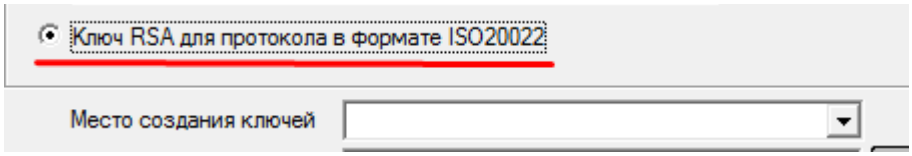


Также рекомендуется установить отметку ***Запоминать и восстанавливать путь к последней папке с ключами***. Это может помочь при поиске ключа на компьютере, если путь к папке с ключами был утерян.

5. Вернитесь на вкладку ***Создание ключей***.



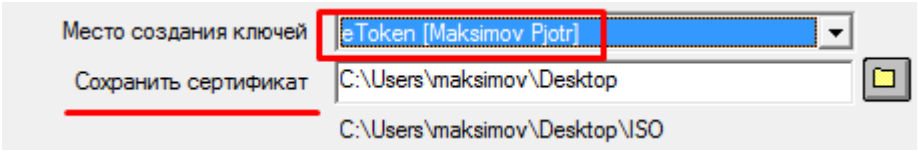
6. Установите отметку ***Ключ RSA для протокола в формате ISO20022.***



7. Выберите место создания **место создания ключей:** «eToken» либо «файл». **Обратите внимание**, что надежнее хранить ключи на токене.

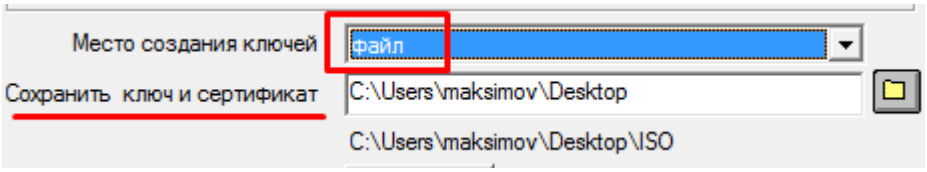
Если ключ создается на токене**,** предварительно убедитесь, что токен подключен к компьютеру.

8. А. **При генерации ключа на токене** заполните поле ***Сохранить сертификат***.



Укажите путь к папке, где будет сохранен **сертификат ключа.**

Б. **При генерации ключа в файле** заполните поле ***Сохранить ключ и сертификат.***

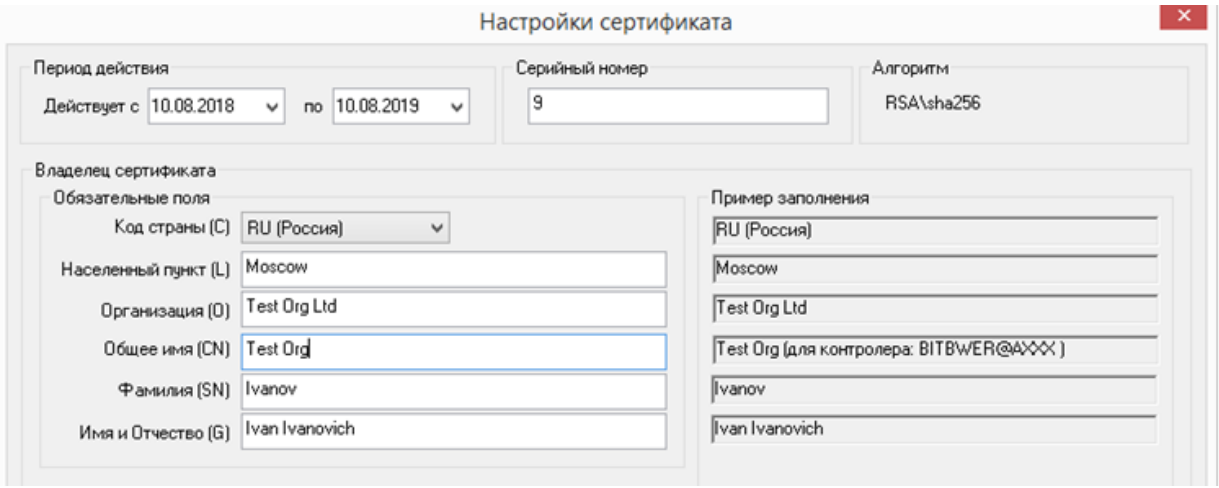


Укажите путь к папке, где будет сохранен **сертификат открытого ключа**.

2.2 Заполнение параметров сертификата

Для настройки параметров сертификата открытого ключа на вкладке ***Создание ключей*** в поле ***Параметры сертификата*** нажмите кнопку ***Настроить.***

Вы перейдете на страницу следующего вида.



Период действия – **у**кажите период действия ключа**,** максимальная длина периода **– 12 месяцев.**

Действует с – дата начала действия сертификата;

По – дата окончания действия сертификата. Начальная и конечная даты входят в период. **Срок действия сертификата устанавливается не более 12 месяцев.**

Серийный номер – серийный номер сертификата, целое число; при настройке параметров очередного сертификата номер автоматически увеличивается на 1.

Заполните параметры в панели ***Владелец сертификата***.

Обратите внимание!

- Необходимо заполнить только первый блок ***Обязательные поля.***
- ***Рекомендуемые поля*** заполнять необязательно**.**
- **Названия всех полей заполняются только на латинице.**

Правила заполнения полей панели ***Владелец сертификата/ Обязательные поля.***

Код страны (C) – наименование страны.

Населенный пункт (L) **–** для юридических лиц укажите населенный пункт, которому принадлежит юридический адрес организации владельца ключа. Для физических лиц укажите населенный пункт регистрации.

Организация(O) **-** введите наименование организации.

Если ключ создается для юридического лица, укажите наименование организации.

Если ключ создается для физического лица, укажите полностью ФИО физического лица, которое является владельцем ключа.

Общее имя (CN) **–** поле можно не заполнять или заполните это поле так же, как и поле ***Организация (O).***

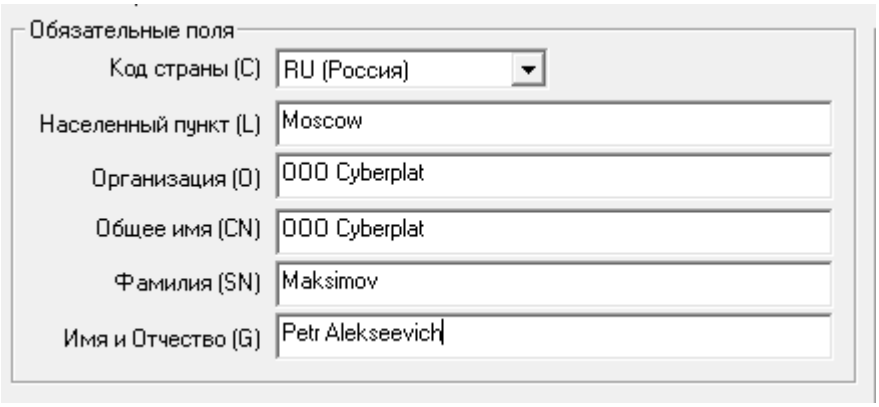
Фамилия (SN) **–** фамилия владельца ключа.

Имя и Отчество (G) – укажите имя и отчество владельца ключа.

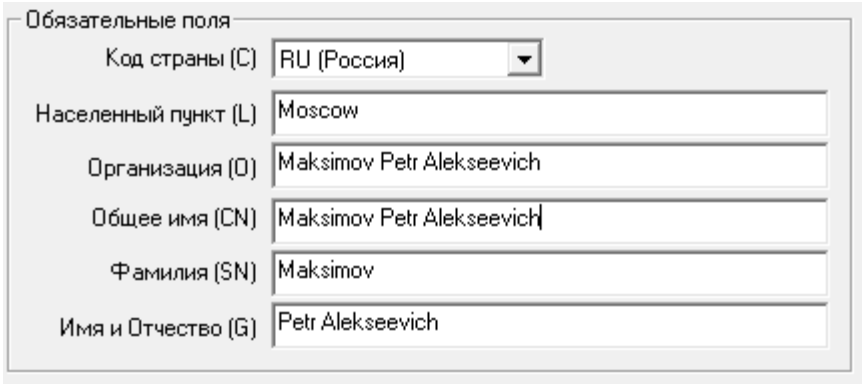
После заполнения всех обязательных полей нажмите кнопку ***ОК.***

Примеры заполнения реквизитов владельца сертификата

Юридические лицо.

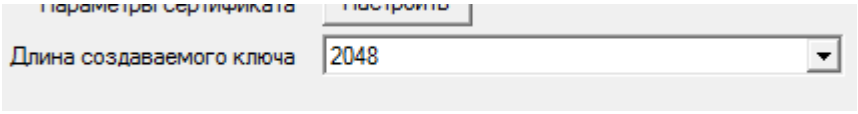


Физическое лицо.

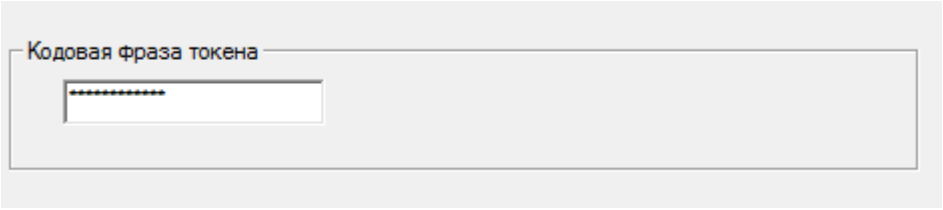


Вернитесь на вкладку ***Создание ключей***.

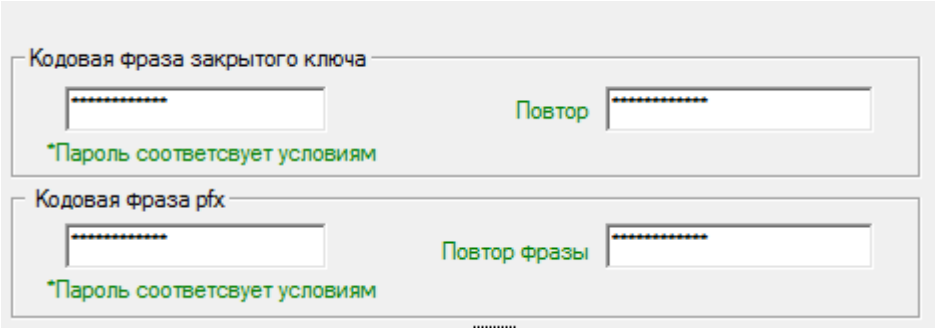
В поле ***Длина создаваемого ключа*** укажите значение **2048.**



При создании ключа **на токене** придумайте и введите ***Кодовую фразу токена.***



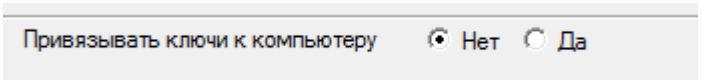
При создании ключа **в файле** введите **единый пароль** в следующие четыре поля.



Требования к паролю: длина не менее 8 символов, пароль должен содержать латинские буквы в верхнем и нижнем регистре**,** цифры, спецсимволы из списка (! @#%).

Внимание! При создании ключа в файле пароль необходимо обязательно заполнить и сохранить. Так как в случе утраты пароля он не подлежит восстановлению и ключ потребуется перевыпускать.

При создании ключа в файле в поле ***Привязывать ключи к компьютеру*** установите отметку **Нет.**



Поле ***Имя ключа в тонком клиенте*** пользователь не заполняет, оно формируется программой Genkey и далее не используется. (Если отметка ***Имя ключа в тонком клиенте*** установлена, то в данном поле автоматически отображается значение, созданное программой Genkey).

Проверьте, что все параметры конфигурации заполнены правильно, и нажмите кнопку ***Создать*.**

Генерация ключей завершена.

В результате генерации будут созданы:

сертификат открытого ключа – файл **certificate.pem** будет создан в файле на диске компьютера,

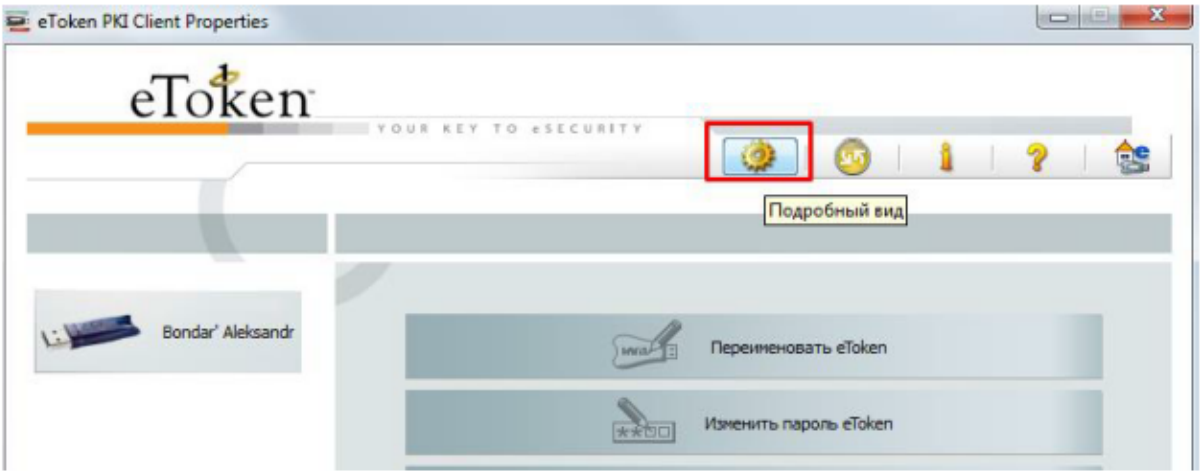
на токене будут созданы **закрытый ключ и pfx-контейнер**, содержащий архив с закрытым ключом и сертификатом ключа.

Файл сертификата открытого ключа **certificate.pem** необходимо заархивировать и отправить по электронной почте в ООО «КИБЕРПЛАТ» по следующим адресам: support@mitacs.com, maksimov@cyberplat.ru, a.titov@cyberplat.ru.

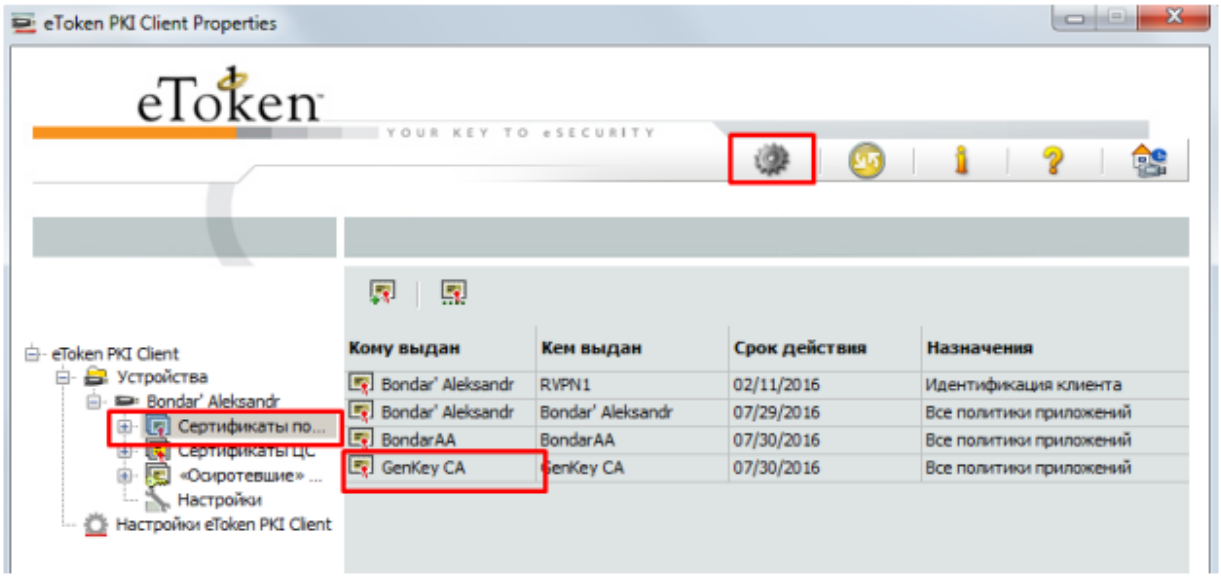
При создании ключа на токене следует удостовериться, что **новый ключ успешно записался на токен**.

Необходимо выполнить следующие действия.

- откройте программу ***PKI Client*** ;
- войдите в пункт главного меню ***Подробный вид;***

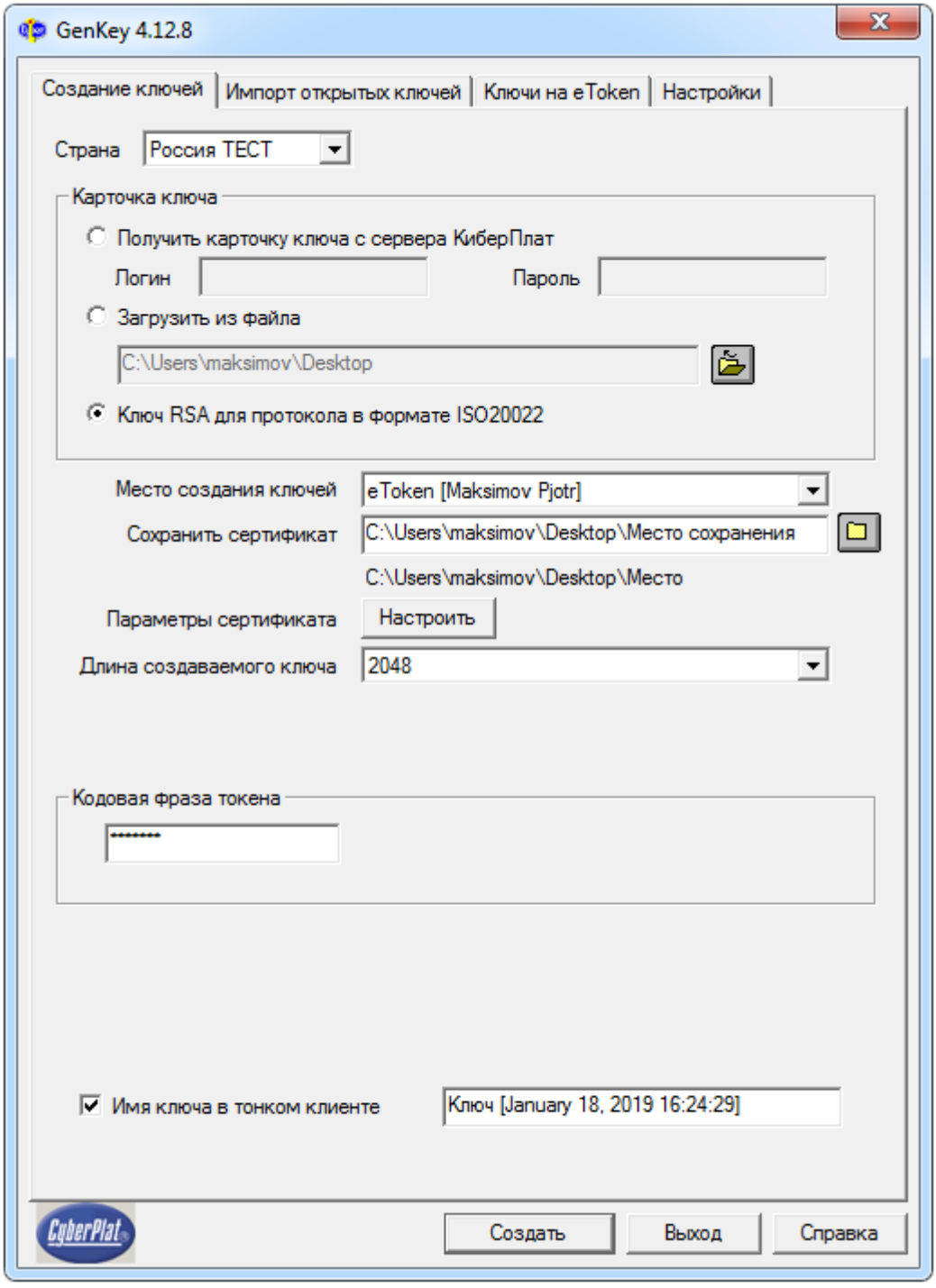


- Проверьте наличие созданного сертификата.



2.3 Пример настроек при создании ключей на токене

На следующем рисунке приведен пример заполнения настроек сертификата при создании ключей на токене.



В поле ***Сохранить сертификат*** указано значение **D:** .

Пусть в настройках сертификата указано название организации **CN= Test Org 2** и дата создания ключей **10.08.2018.**

Тогда сертификат открытого ключа будет создан на диске компьютера в папке **D:\Test Org 2_180810.** Это название отображается ниже поля ***Сохранить сертификат*.**

Имена созданных файлов:

Test Org 2_180810_certificate.pem – файл сертификата открытого ключа, сохраняется в созданной папке;

Test Org 2_180810_certificate.pfx – файл хранилища сертификата, сохраняется на токене;

Test Org 2_180810_private_key.pem – файл закрытого ключа, сохраняется на токене.

2.4 Создание ключей в файле

Ключи необходимо выпускать для лиц, обладающих **полномочиями подписантов**.

Порядок создания ключей на токене описан в одноименном разделе.

Порядок создания ключей в файле аналогичен порядку создания ключей на токене. Ключи могут размещаться на **жестком диске компьютера** или на **флеш-носителе**. В файлах сохраняются сертификат открытого ключа и закрытый ключ.

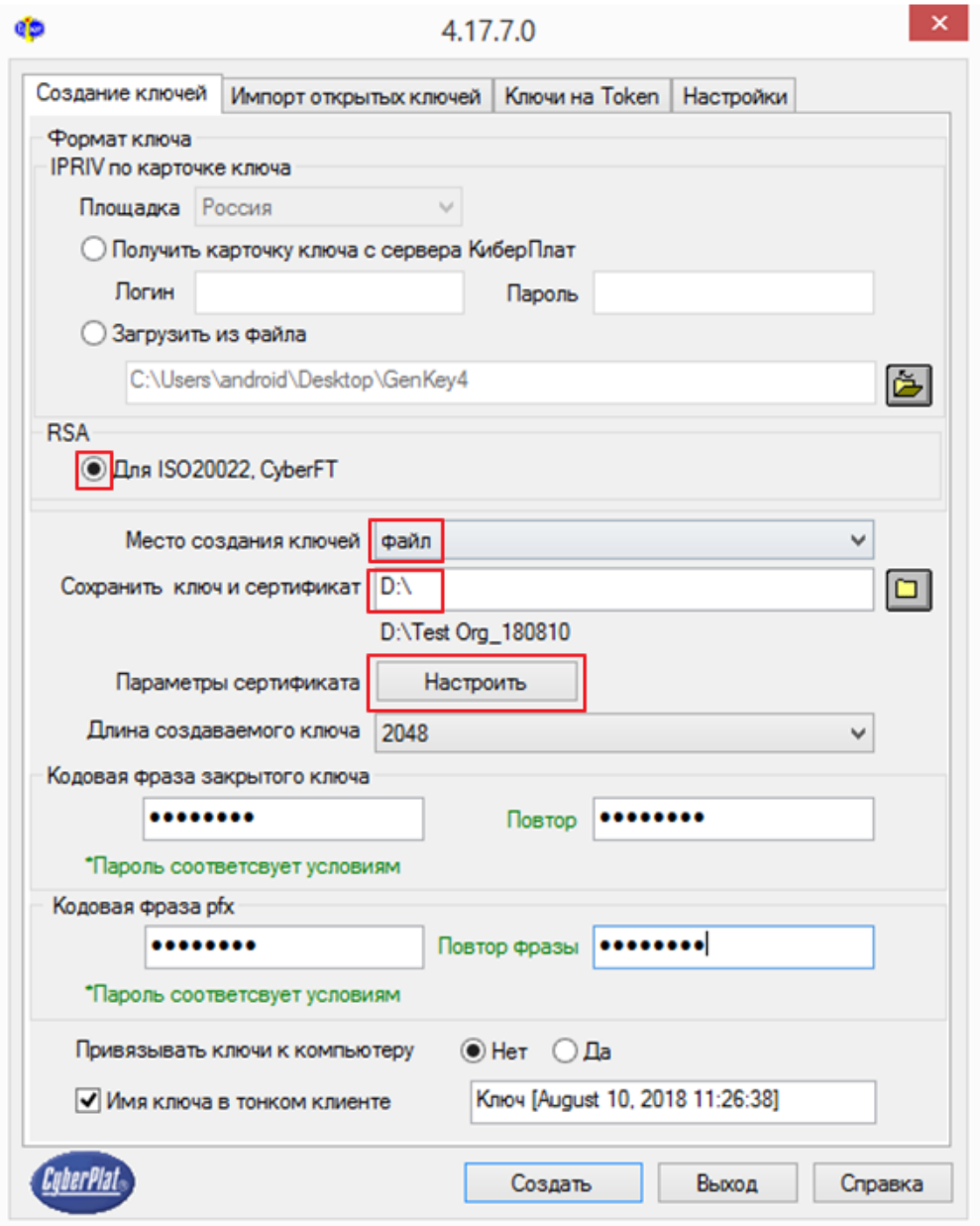
Порядок работы при создании ключей в файле

1. Запустите программу генерации ключей GenKey.
2. Заполните параметры, отмеченные на рисунке красной рамкой.

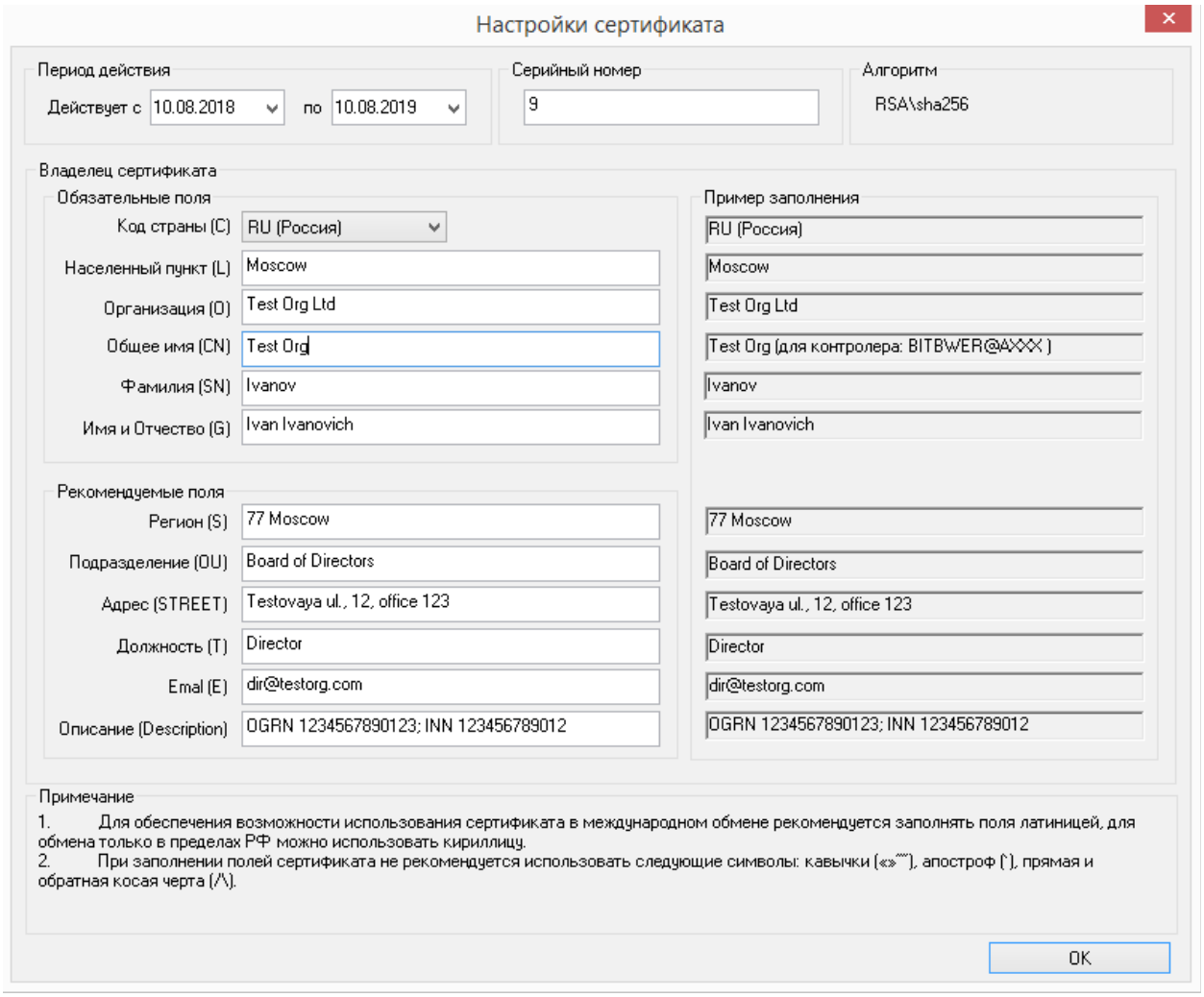
   Установите отметку ***RSA.***

   Место создания ключей – выберите значение «файл».

   В поле ***Сохранить ключи и сертификат*** укажите путь к папке, куда будут сохраняться ключи. Название создаваемой папки с ключами отображается ниже поля.



3. В поле ***Параметры сертификата*** нажмите кнопку ***Настроить***, откроется следующее окно.



Заполните ***Период действия ключей.***

Внимание!

Максимальный срок действия ключа **12 месяцев**.

Надо **заполнить все обязательные поля** владельца сертификата, как это описано в разделе «Заполнение параметров сертификата».

4. Вернитесь на вкладку ***Создание ключей***. Установите длину ключа **2048 бит**.

Установите длину ключа **2048 бит**.

В параметре ***Привязывать ключи к компьютеру*** установите отметку **«Нет».**

5. Далее необходимо указать ***одинаковые кодовые фразы*** (пароли) для закрытого ключа и для хранилища ключа PFX.

   Внимание! **Кодовую фразу необходимо сохранить**. Так как в случае утраты пароль не подлежит восстановлению, ключ потребуется перевыпускать.

6. После заполнения параметров нажмите кнопку ***Создать***.

7. В папке, путь к которой указан в поле ***Сохранить файл и сертификат,*** появится новая папка с файлами, перечисленными ниже.

Название папки формируется из значения поля ***Общее имя (CN)*** в настройках сертификата и даты создания ключей в формате ГГММДД.

Пример. CN= Test Org, дата создания ключей 10.08.2018.

Имя созданной папки: **Test Org_180810**

Имена файлов, сохраняемых в созданной папке:

Test Org_180810_certificate.pem – файл сертификата открытого ключа;

Test Org_180810_certificate.pfx – файл хранилища сертификата открытого ключа;

Test Org_180810_private_key.pem – файл закрытого ключа.

Внимание! Обязательно сохраните созданные файлы. Они необходимы для подписания отправляемых документов.

Файл **сертификата открытого ключа** необходимо отправить по электронной почте в ООО «КИБЕРПЛАТ» по следующим адресам:

- support@cyberplat.ru ,
- maksimov@cyberplat.ru,
- a.titov@cyberplat.ru.

3 Подготовка Акта о признании электронной подписи

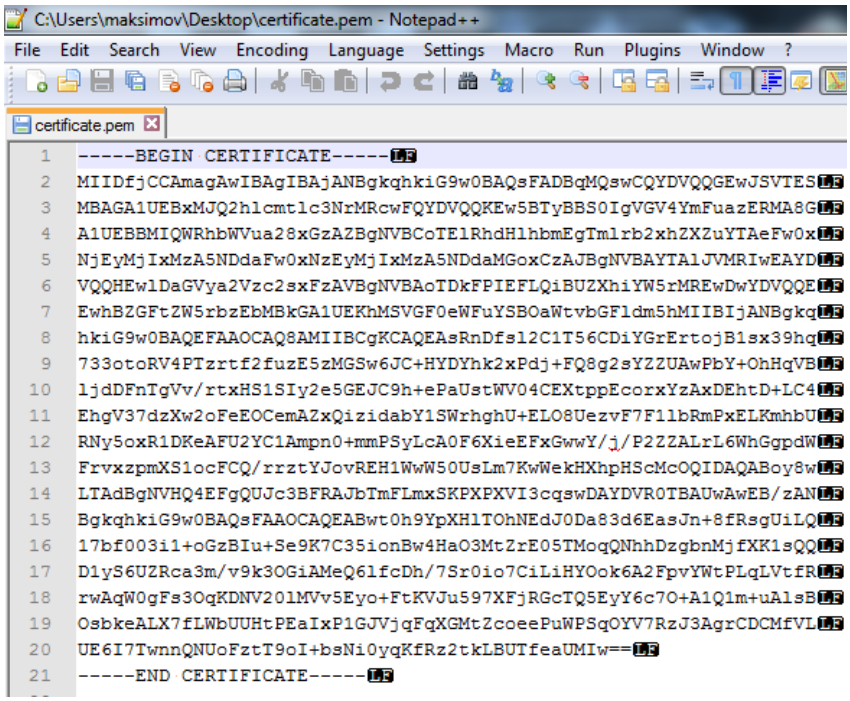
3.1 Проверка сертификата

Условием возможности работы Клиента с банком ООО КБ «ПЛАТИНА» является подписание **Акта о признании электронной подписи** (далее по тексту «Акт»).
Для каждого ключа, регистрируемого в системе CyberFT, необходимо сформировать и подписать Акт.
Шаблон Акта вы можете скачать здесь:
http://download.cyberft.ru/Documentation/Acts/170406%20Podpisant%20DBO.doc .

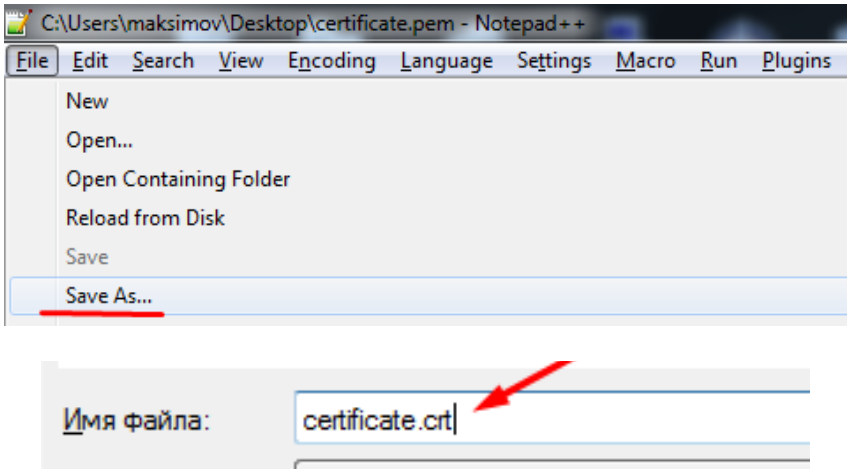
В данном разделе описан **порядок подготовки текста Акта**.

Изменение расширения файла сертификата.
Для просмотра реквизитов сертификата средствами стандартного ПО просмотра сертификатов файл сертификата должен иметь расширение **cer** или **crt**.
Сертификаты подписантов, созданные с помощью ПО GenKey, обычно имеют расширение **pem**.
Чтобы изменить расширение, необходимо открыть файл с помощью ПО Notepad (Блокнот) или любого другого текстового редактора.

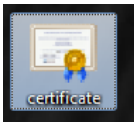
На экран будет выведено содержимое сертификата следующего вида.



Для изменения расширения войдите в пункт меню ***Файл (File)***, выберите команду ***Сохранить как (Save as)***, измените расширение файла **pem** на **crt** или **cer** и сохраните файл.



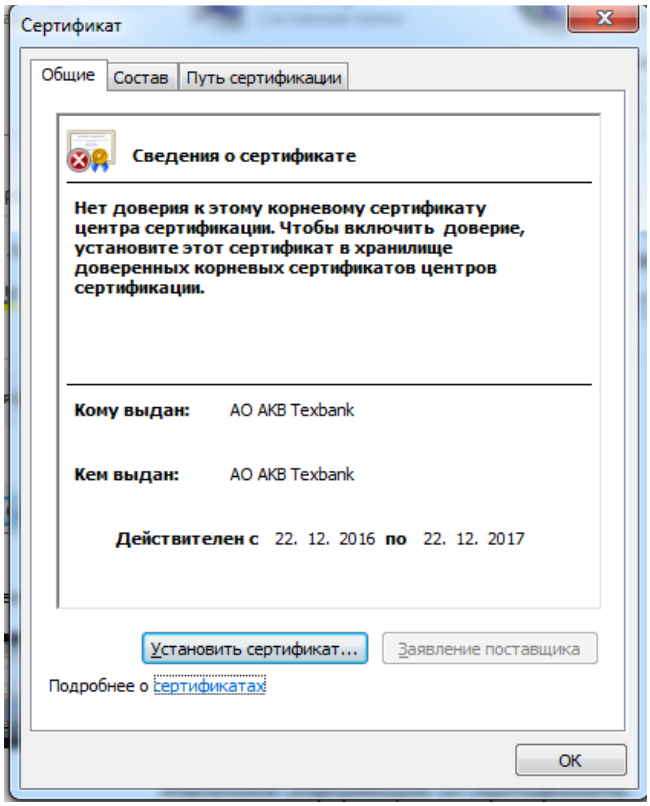
Сохраненный файл сертификата должен иметь следующий вид.



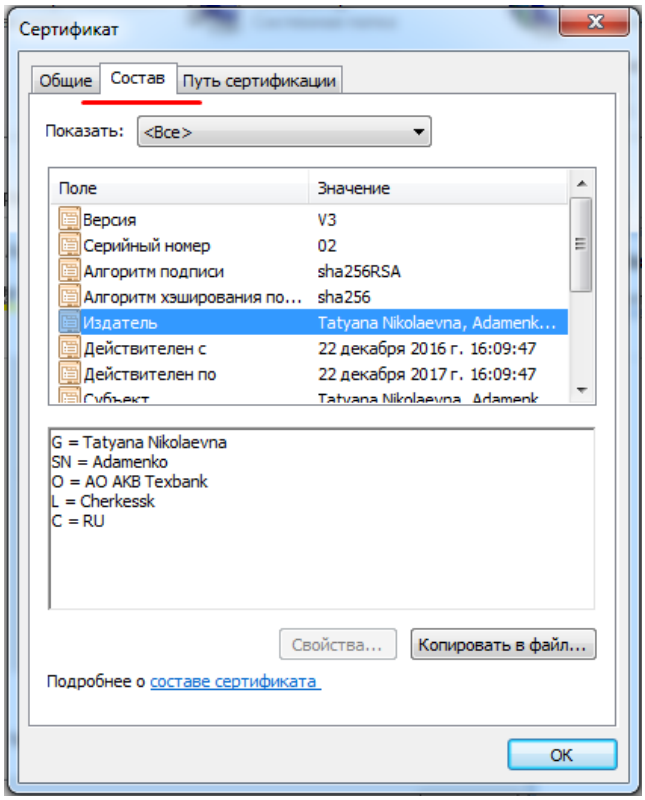
3.2 Заполнение реквизитов акта

Копирование реквизитов сертификата в Акт.
Для просмотра реквизитов сертификата откройте изменённый файл сертификата.

Откроется следующее окно.

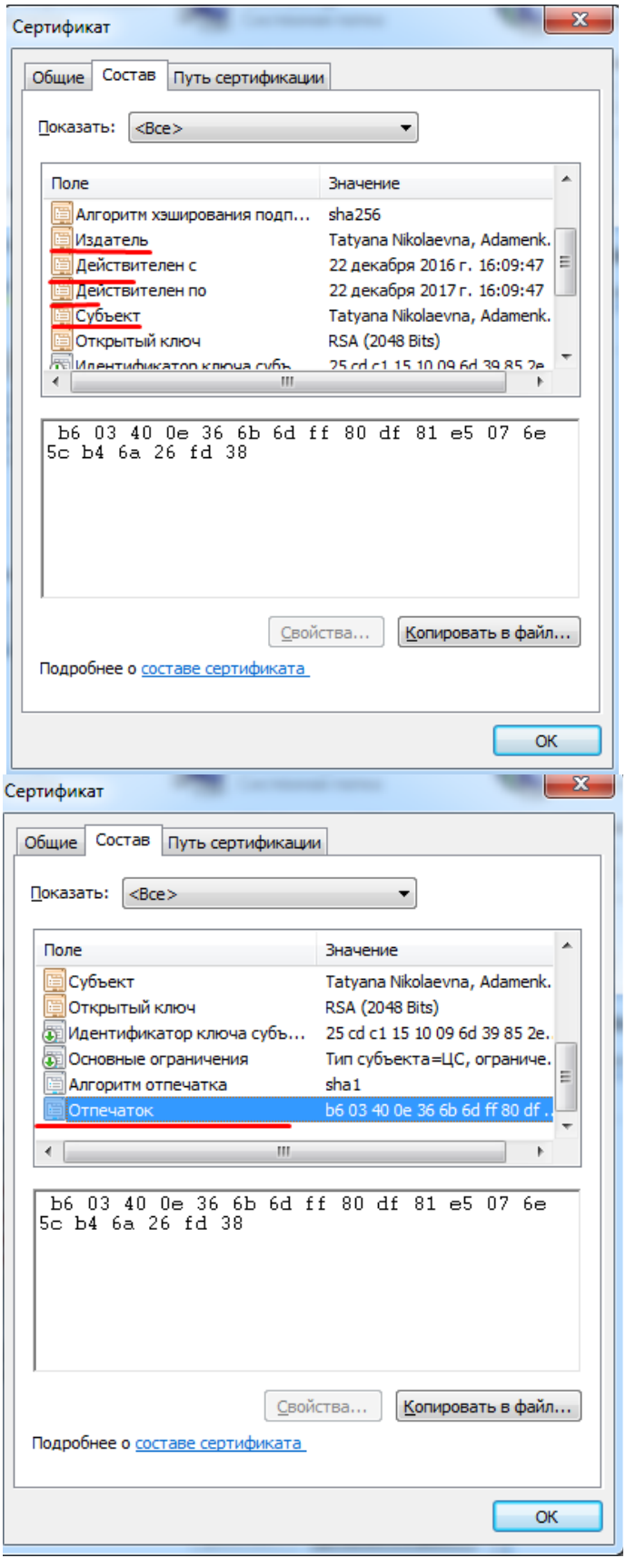


Перейдите на вкладку ***Состав***.



Из показанного окна вы будете переносить с помощью копирования **реквизиты сертификата в Акт.**

Надо перенести значения реквизитов: ***Издатель, Действителен с, Действителен по, Субъект*** и ***Отпечаток.***



Скачайте шаблон Акта о признании электронной подписи:

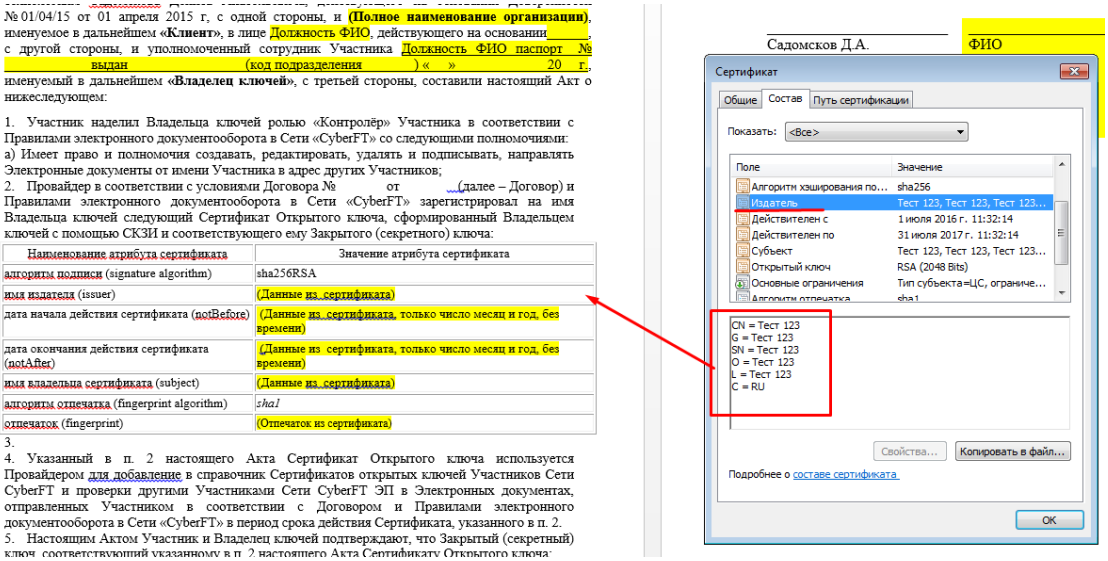
http://download.cyberft.ru/Documentation/Acts/170406%20Podpisant%20DBO.doc.

Внимание! Копируйте и переносите в шаблон Акта всё содержимое перечисленных параметров **за исключением дат** начала действия и окончания сертификата. В датах не переносится время, необходимо перенести только число, месяц, год.

На следующих рисунках в левой части выделены строки таблицы из Акта, в правой части показаны атрибуты сертификата. В списке полей в сертификате выбирается реквизит, в нижней части окна показано значение реквизита, которое копируется в таблицу в Акте.

(Для просмотра рисунков можно изменить масштаб отображения документа.)

1 ***Имя издателя*** – скопируйте значение атрибута ***Издатель*** из нижней части страницы.



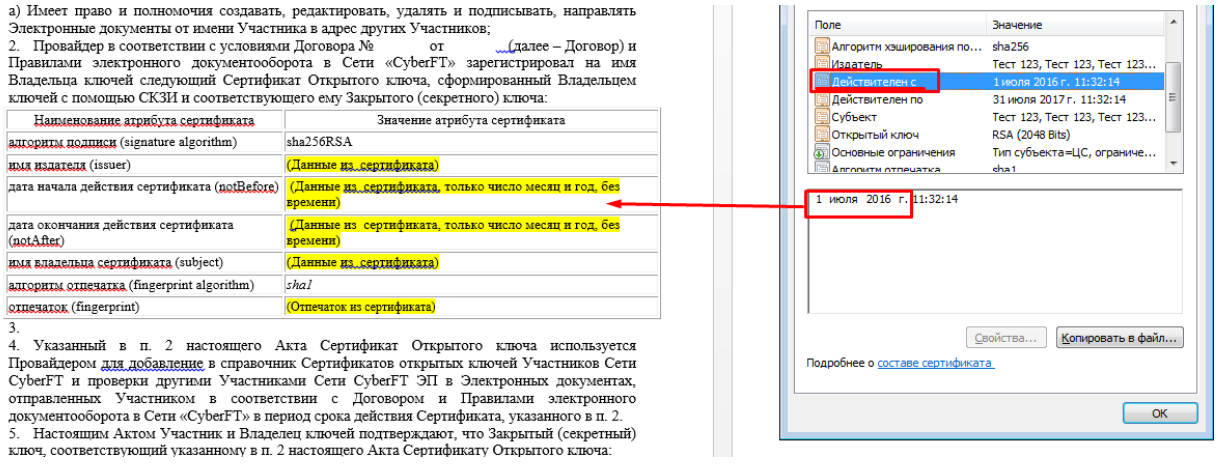
№ 01/04/15 от 01 апреля 2015 г, с одной стороны, и **(Полное наименование организации)**, именуемое в дальнейшем **«Клиент»**, в лице Должность ФИО, действующего на основании_____, с другой стороны, и уполномоченный сотрудник Участника Должность ФИО паспорт № выдан (код подразделения) « » 20 г., именуемый в дальнейшем **«Владелец ключей»**, с третьей стороны, составили настоящий Акт о нижеследующем:

1. Участник наделил Владельца ключей ролью «Контролёр» Участника в соответствии с Правилами электронного документооборота в Сети «CyberFT» со следующими полномочиями:
а) Имеет право и полномочия создавать, редактировать, удалять и подписывать, направлять Электронные документы от имени Участника в адрес других Участников;
2. Провайдер в соответствии с условиями Договора № от (далее – Договор) и Правилами электронного документооборота в Сети «CyberFT» зарегистрировал на имя Владельца ключей следующий Сертификат Открытого ключа, сформированный Владельцем ключей с помощью СКЗИ и соответствующего ему Закрытого (секретного) ключа:

Наименование атрибута сертификата	Значение атрибута сертификата
алгоритм подписи (signature algorithm)	sha256RSA
имя издателя (issuer)	(Данные из сертификата)
дата начала действия сертификата (notBefore)	(Данные из сертификата, только число месяц и год, без времени)
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)
имя владельца сертификата (subject)	(Данные из сертификата)
алгоритм отпечатка (fingerprint algorithm)	*sha1*
отпечаток (fingerprint)	(Отпечаток из сертификата)

3.
4. Указанный в п. 2 настоящего Акта Сертификат Открытого ключа используется Провайдером для добавление в справочник Сертификатов открытых ключей Участников Сети CyberFT и проверки другими Участниками Сети CyberFT ЭП в Электронных документах, отправленных Участником в соответствии с Договором и Правилами электронного документооборота в Сети «CyberFT» в период срока действия Сертификата, указанного в п. 2.
5. Настоящим Актом Участник и Владелец ключей подтверждают, что Закрытый (секретный) ключ, соответствующий указанному в п. 2 настоящего Акта Сертификату Открытого ключа:

2 ***Действителен с*** – скопируйте день, месяц, год (без значения времени).

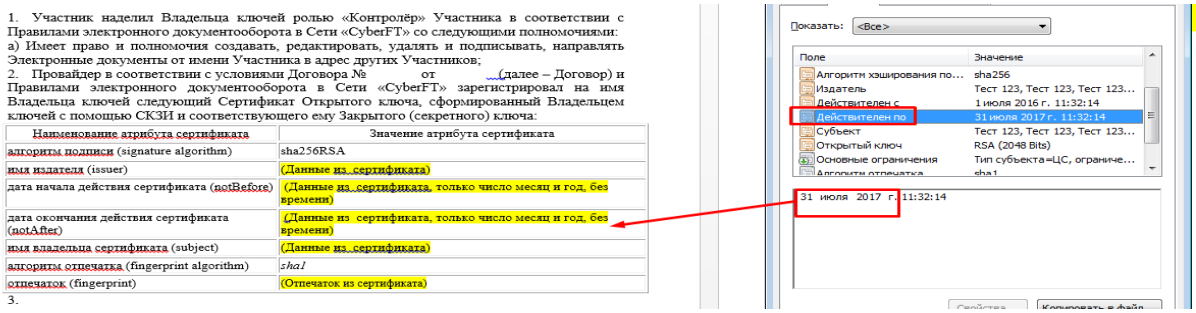


а) Имеет право и полномочия создавать, редактировать, удалять и подписывать, направлять Электронные документы от имени Участника в адрес других Участников;
2. Провайдер в соответствии с условиями Договора № от (далее – Договор) и Правилами электронного документооборота в Сети «CyberFT» зарегистрировал на имя Владельца ключей следующий Сертификат Открытого ключа, сформированный Владельцем ключей с помощью СКЗИ и соответствующего ему Закрытого (секретного) ключа:

Наименование атрибута сертификата	Значение атрибута сертификата
алгоритм подписи (signature algorithm)	sha256RSA
имя издателя (issuer)	(Данные из сертификата)
дата начала действия сертификата (notBefore)	(Данные из сертификата, только число месяц и год, без времени)
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)
имя владельца сертификата (subject)	(Данные из сертификата)
алгоритм отпечатка (fingerprint algorithm)	*sha1*
отпечаток (fingerprint)	(Отпечаток из сертификата)

3.
4. Указанный в п. 2 настоящего Акта Сертификат Открытого ключа используется Провайдером для добавление в справочник Сертификатов открытых ключей Участников Сети CyberFT и проверки другими Участниками Сети CyberFT ЭП в Электронных документах, отправленных Участником в соответствии с Договором и Правилами электронного документооборота в Сети «CyberFT» в период срока действия Сертификата, указанного в п. 2.
5. Настоящим Актом Участник и Владелец ключей подтверждают, что Закрытый (секретный) ключ, соответствующий указанному в п. 2 настоящего Акта Сертификату Открытого ключа:

3 ***Действителен по*** – скопируйте день, месяц, год.



1. Участник наделил Владельца ключей ролью «Контролёр» Участника в соответствии с Правилами электронного документооборота в Сети «CyberFT» со следующими полномочиями:
а) Имеет право и полномочия создавать, редактировать, удалять и подписывать, направлять Электронные документы от имени Участника в адрес других Участников;
2. Провайдер в соответствии с условиями Договора № от (далее – Договор) и Правилами электронного документооборота в Сети «CyberFT» зарегистрировал на имя Владельца ключей следующий Сертификат Открытого ключа, сформированный Владельцем ключей с помощью СКЗИ и соответствующего ему Закрытого (секретного) ключа:

Наименование атрибута сертификата	Значение атрибута сертификата
алгоритм подписи (signature algorithm)	sha256RSA
имя издателя (issuer)	(Данные из сертификата)
дата начала действия сертификата (notBefore)	(Данные из сертификата, только число месяц и год, без времени)
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)
имя владельца сертификата (subject)	(Данные из сертификата)
алгоритм отпечатка (fingerprint algorithm)	*sha1*
отпечаток (fingerprint)	(Отпечаток из сертификата)

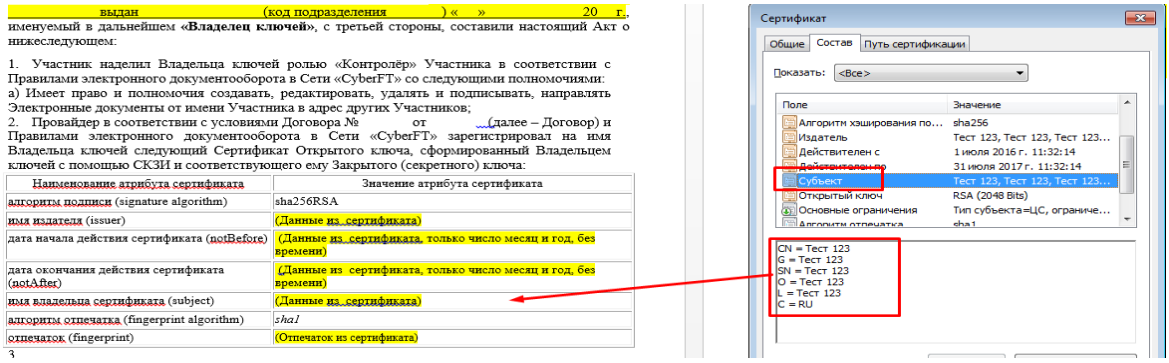
3.

Показать: <Все>

Поле	Значение
Алгоритм хэширования по...	sha256
Издатель	Тест 123, Тест 123, Тест 123...
Действителен с	1 июля 2016 г. 11:32:14
Действителен по	31 июля 2017 г. 11:32:14
Субъект	Тест 123, Тест 123, Тест 123...
Открытый ключ	RSA (2048 Bits)
Основные ограничения	Тип субъекта=ЦС, ограниче...
Алгоритм отпечатка	sha1

31 июля 2017 г. 11:32:14

4 ***Имя владельца сертификата*** – скопируйте значение реквизита ***Субъект***.



выдан (код подразделения) « » 20 г.,
именуемый в дальнейшем **«Владелец ключей»**, с третьей стороны, составили настоящий Акт о нижеследующем:

1. Участник наделил Владельца ключей ролью «Контролёр» Участника в соответствии с Правилами электронного документооборота в Сети «CyberFT» со следующими полномочиями:
а) Имеет право и полномочия создавать, редактировать, удалять и подписывать, направлять Электронные документы от имени Участника в адрес других Участников;
2. Провайдер в соответствии с условиями Договора № от (далее – Договор) и Правилами электронного документооборота в Сети «CyberFT» зарегистрировал на имя Владельца ключей следующий Сертификат Открытого ключа, сформированный Владельцем ключей с помощью СКЗИ и соответствующего ему Закрытого (секретного) ключа:

Наименование атрибута сертификата	Значение атрибута сертификата
алгоритм подписи (signature algorithm)	sha256RSA
имя издателя (issuer)	(Данные из сертификата)
дата начала действия сертификата (notBefore)	(Данные из сертификата, только число месяц и год, без времени)
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)
имя владельца сертификата (subject)	(Данные из сертификата)
алгоритм отпечатка (fingerprint algorithm)	*sha1*
отпечаток (fingerprint)	(Отпечаток из сертификата)

3

Сертификат

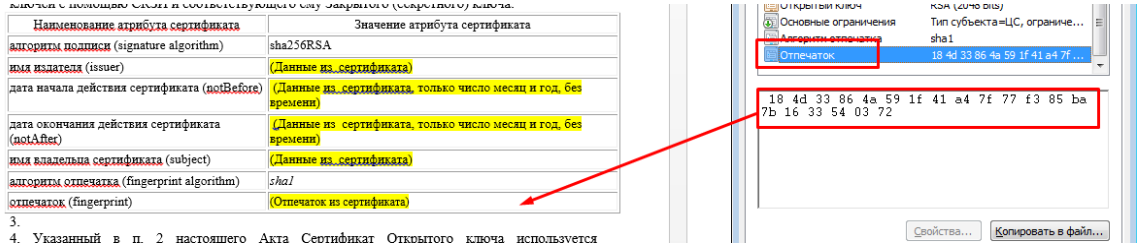
Общие | Состав | Путь сертификации

Показать: <Все>

Поле	Значение
Алгоритм хэширования по...	sha256
Издатель	Тест 123, Тест 123, Тест 123...
Действителен с	1 июля 2016 г. 11:32:14
Действителен по	31 июля 2017 г. 11:32:14
Субъект	Тест 123, Тест 123, Тест 123...
Открытый ключ	RSA (2048 Bits)
Основные ограничения	Тип субъекта=ЦС, ограниче...
Алгоритм отпечатка	sha1

CN = Тест 123
G = Тест 123
SN = Тест 123
O = Тест 123
L = Тест 123
C = RU

5 ***Отпечаток сертификата*** – скопируйте значение атрибута ***Отпечаток***.



Наименование атрибута сертификата	Значение атрибута сертификата
алгоритм подписи (signature algorithm)	sha256RSA
имя издателя (issuer)	(Данные из сертификата)
дата начала действия сертификата (notBefore)	(Данные из сертификата, только число месяц и год, без времени)
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)
имя владельца сертификата (subject)	(Данные из сертификата)
алгоритм отпечатка (fingerprint algorithm)	*sha1*
отпечаток (fingerprint)	(Отпечаток из сертификата)

3.
4. Указанный в п. 2 настоящего Акта Сертификат Открытого ключа используется

Основные ограничения | Тип субъекта=ЦС, ограниче...
Алгоритм отпечатка | sha1
Отпечаток | 18 4d 33 86 4a 59 1f 41 a4 7f...

18 4d 33 86 4a 59 1f 41 a4 7f 77 f3 85 ba
7b 16 33 54 03 72

Свойства... | Копировать в файл...

Пример заполнения таблицы в акте

Наименование реквизита сертификата	Значение реквизита сертификата
Алгоритм подписи (signature algorithm)	sha256RSA
Имя издателя (issuer)	CN = TEST TEST TEST. O = CyberFT L = Moscow S = Moscow C = RU
Дата начала действия сертификата (notBefore)	12 мая 2017 г.
Дата окончания действия сертификата (notAfter)	11 мая 2018 г.

Наименование реквизита сертификата	Значение реквизита сертификата
Имя владельца сертификата (subject)	CN = TEST TEST TEST. O = CyberFT L = Moscow S = Moscow C = RU
Алгоритм отпечатка (fingerprint algorithm)	sha1
Отпечаток (fingerprint)	1 a1 a1a1 1a2a2a 22a3в3 в3в3 па5а 5а п5

Внимание!

Сохраненный после создания **сертификат ключа (файл certificate.pem\crt) и акт в формате doc** необходимо заархивировать и выслать на следующие адреса**:**

maksimov@cyberplat.ru, a.titov@cyberplat.ru, support@cyberplat.ru **.**

В теме письма укажите наименование компании клиента, в теле письма напишите «Новый ключ подписанта и акт признания ЭП, на проверку».

4 Установка программы для подписания отправляемых документов.

Далее необходимо установить программу **CyberSignService** подписания отправляемых документов.

Скачайте установочный файл здесь:

http://download.cyberft.ru/CyberSignService/ .

Программа устанавливается пользователем с правами администратора компьютера.

Инструкцию по настройке программы можно посмотреть в документе [6], а также на сайте https://www.cyberft.ru/ в разделе Главная/ Документы и ПО/ Программное обеспечение (https://cyberft.ru/downloads/soft) по ссылке «Руководство «Сервис подписания в сети CyberFT».

5 Документация

Ссылки на документацию ПО «Терминал CyberFT» вы найдете здесь: https://cyberft.ru/downloads/soft .

Комплект документации для работы с Терминалом сети CyberFT включает в себя следующие документы.

1. Терминал сети CyberFT. Руководство администратора. ООО «КИБЕРПЛАТ», 2018.
2. Терминал сети CyberFT. Руководство пользователя. ООО «КИБЕРПЛАТ», 2018.

3. Терминал сети CyberFT. Руководство по установке. ООО «КИБЕРПЛАТ», 2018.
4. Порядок подключения к процессингу CyberFT. Руководство администратора. ООО «КИБЕРПЛАТ», 2018.
5. Создание ключа подписанта системы CyberFT с помощью Genkey. Руководство пользователя. ООО «КИБЕРПЛАТ», 2019.
6. Сервис подписания в сети CyberFT. Руководство пользователя. ООО «КИБЕРПЛАТ», 2018.

В документе [1] приведен список терминов и сокращений, используемых в документации.