**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 контролёра и подписанта для системы CyberFT.

Руководство администратора.

2017

# Аннотация

В настоящем документе описан процесс создания ключей контролёра и комплекта ключей подписанта. Данные ключи необходимы для формирования защищённого подключения, и шифрования, для выполнения межбанковского документооборота по системе CyberFT.

# Содержание

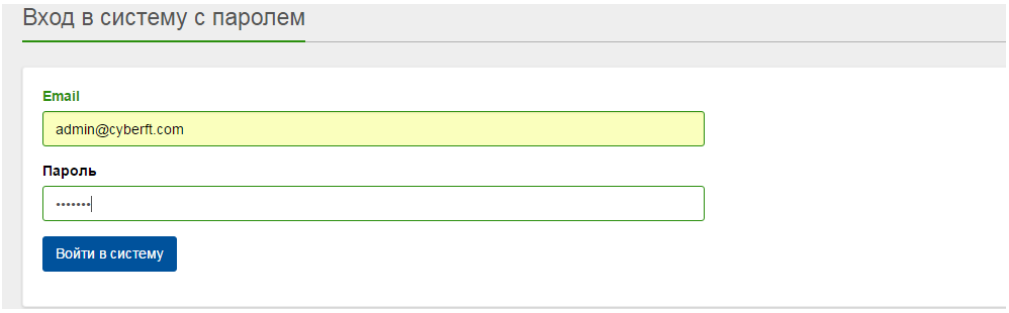
# 1 Создание ключа контролёра и подготовка актов.

## 1.1. Авторизация.

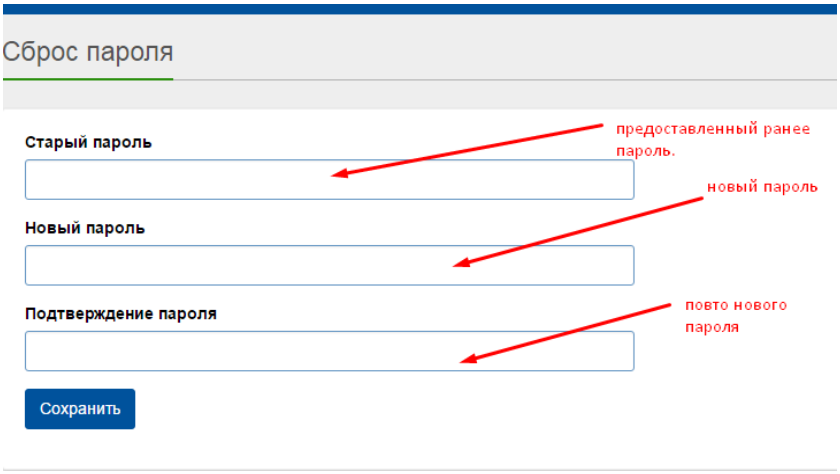
Для создания ключа контролёра вам необходимо авторизоваться под пользователем с правами администратора по данному адресу:

https://cyberft-term.cyberplat.ru

**Данные для доступа были предоставлены при первом подключении к CyberFT.**




Потребуется установка нового пароля:

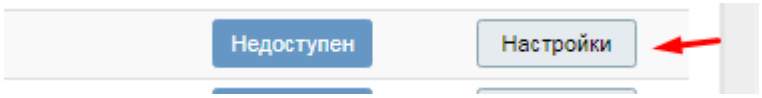


### 1.2. Создание ключа контролера.

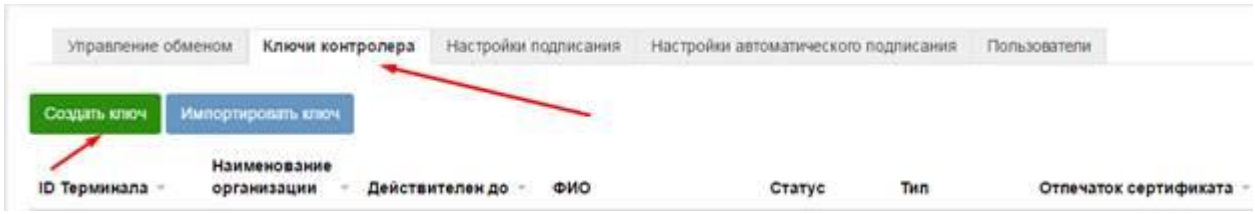
**Ключ контролера необходим только один. Владельцем ключа контролера может быть только: генеральный директор, председатель правления, заместитель председателя правления.**

Для создания ключа контролёра необходимо, зайти в раздел «**Настройки**» далее «**Терминалы**»:

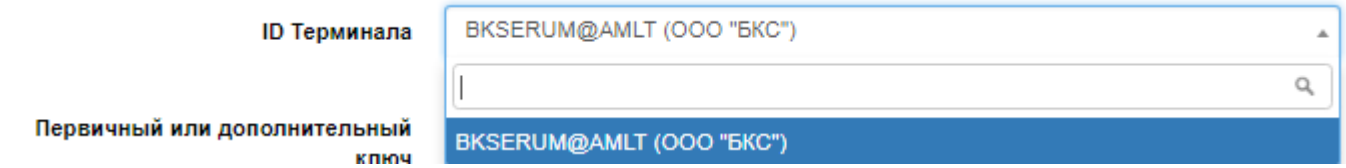

Будет предоставлен список доступных вам терминалов, выбираем необходимый для которого создаётся ключ, нажимаем «**настройки**»:




Выбираем вкладку «**Ключи контролёра**» далее нажимаем создать ключ:



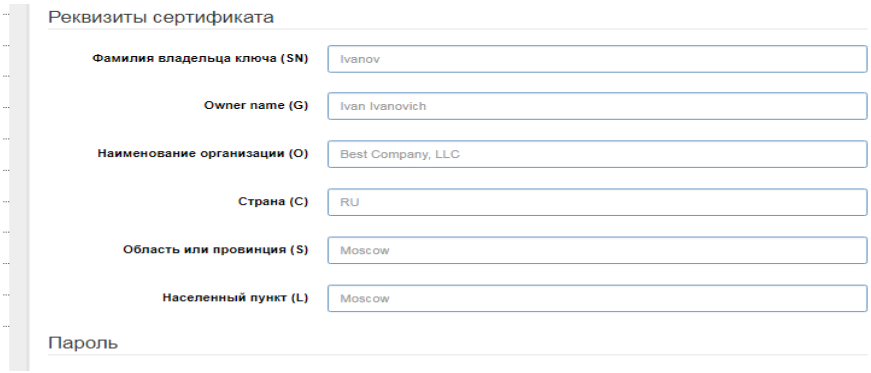

Выбираем ID необходимого вам терминала.




**«Первичный или дополнительный ключ»** ставим **«Первичный».**


**«Личный ключ/Ключ организации»** ставим **«Ключ организации»**


**Далее заполняем реквизиты.**



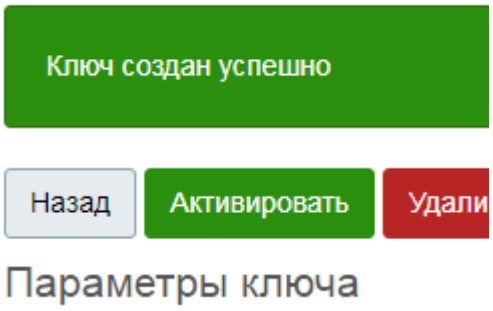

Далее вводим и подтверждаем пароль.

**Обязательно! Запомните и по возможности сохраните\запишите данный пароль. Он потребуется для запуска терминала.**

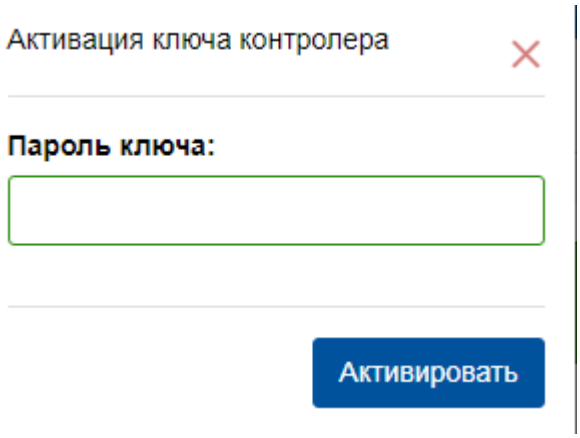
**Данный пароль, восстановлению не подлежит.**

После того как ключ будет создан, откроется окно «параметры ключа».

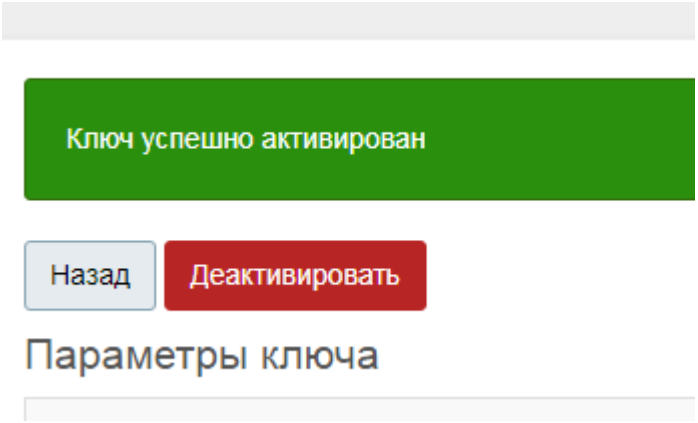
Сверху будет кнопка активировать, необходимо нажать на неё.




Ввести пароль придуманный при создании ключа. Нажать активировать.



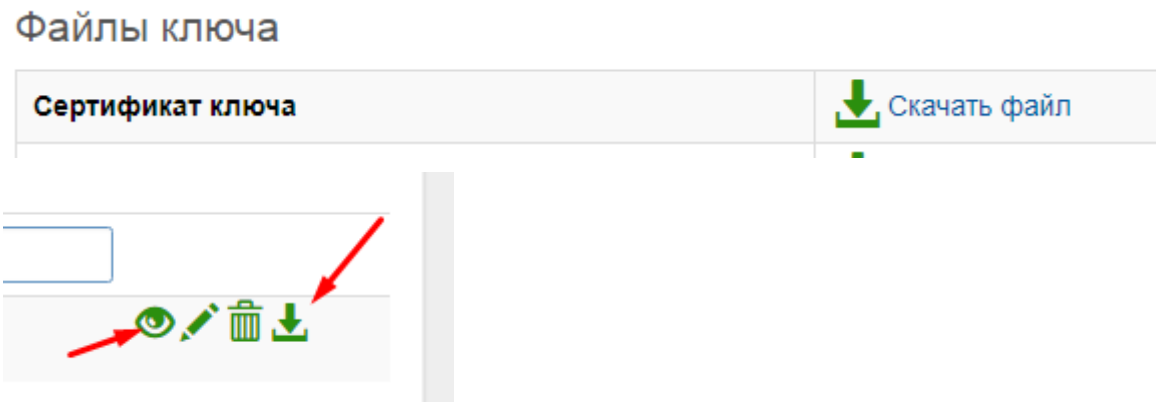
Если пароль был введен верно, буде отображено сообщение, что ключ успешно активирован:




### 1.3. Скачиваем сертификат ключа.

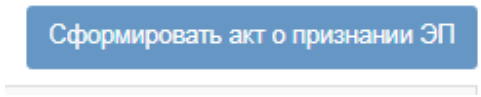
После того как ключ будет создан у вас откроется окно с данными ключа, изображение ниже.

Если окно закрыли, зайти можно через «**Настройки**» далее «**Терминалы**» будет предоставлен список доступных вам терминалов, выбираем необходимый терминал для которого создаётся ключ, нажимаем «**настройки**», выбираем вкладку «**Ключи контролёра**», выбираем ключ нажимаем на просмотр либо сразу скачать файл сертификата:



### 1.4. Подготовка акта признания.

Нажимаем**: «Сформировать акт о призвании ЭП»** и заполняем поля**.**



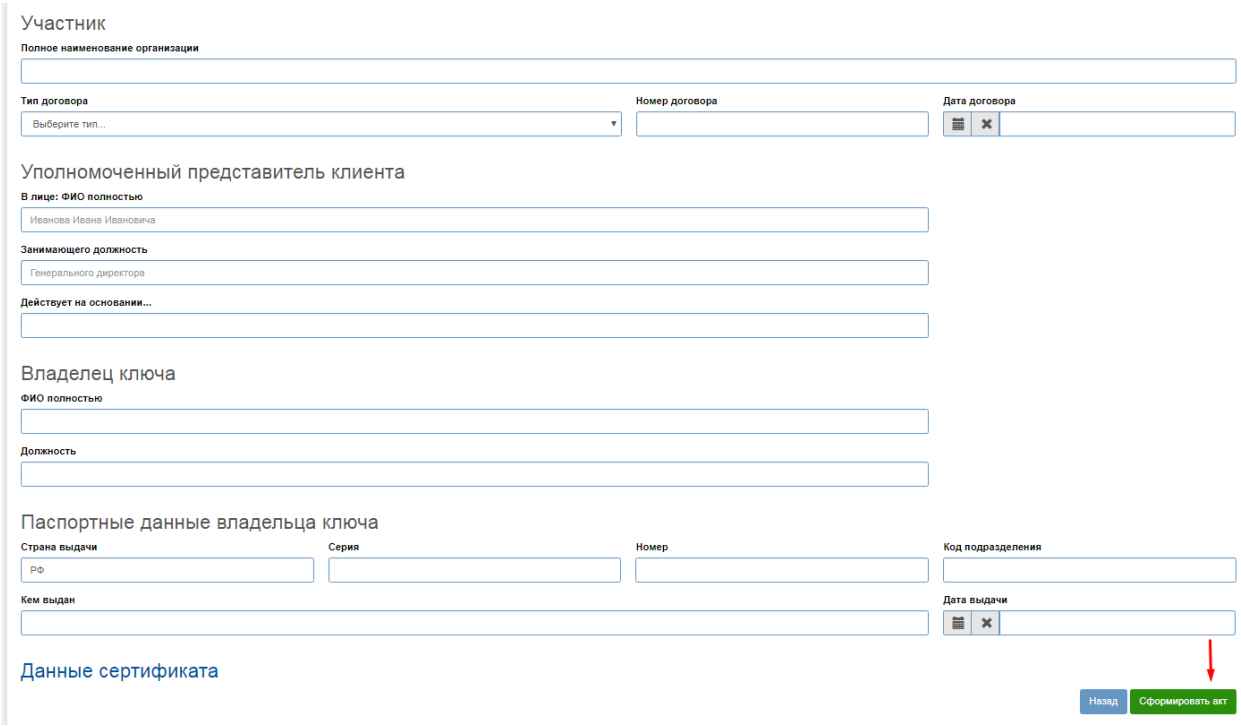

**Внимание! Номер договора и дату договора не заполняете, данная ифнормация будет заполнена на стороне Банка.**

Если у вас планируется только получение выписок выбираем тип договора:

**«ИНФОРМАЦИОННОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ».**

Если планируется полная работа со счетом, отправка платёжных поручений, документов и т.д в Банк. Тогда выбираете тип договора:

**«ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ »**




**<u>Внимание!</u> Сформированный акт, в электронном виде в формате «.doc» и файл сертификата ключа, который был скачен ранее, оправить на данный адрес в архиве: cyberft@platina.ru**

**<u>Обязательно!</u> В *теме письма* укажите наименование вашей организации. Это поможет ускорить проверку ваших актов и сертификатов.**

В теме написать, наименование компании, в теле письма написать «Новый ключ контролёра и акт признания ЭП, для проверки».

# 2 Создание ключа подписанта и подготовка актов.

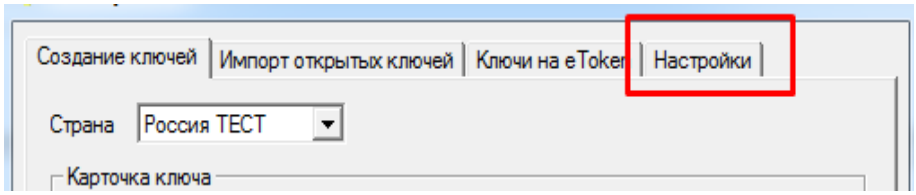
## 2.1 Скачивание программы GenKey.

Дистрибутив программы скачать можно по данному адресу –

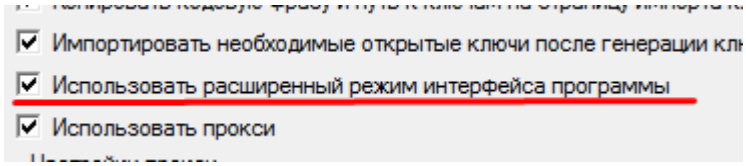
http://download.cyberft.ru/GenKey/GenKey.zip

Запускаем программу.

Переходим во вкладку «**Настройки**»:

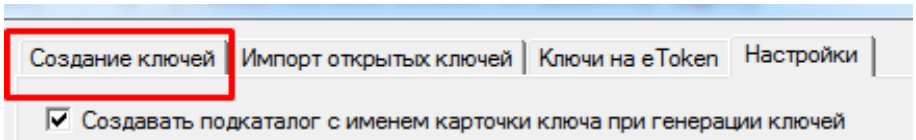



Устанавлвиваем парметр **«Использовать расширенный режим интерфейса»:**

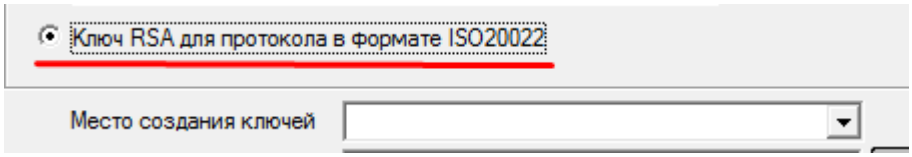



Так же реокомендую поставить парметр «**Запоминать и восстанавливать путь к последней папке с ключами**», это может помочь с поиском ключа на комипьютере, если путь сохранения был утерян.

Возвращаемся во вкладку «**Создание ключей**»:



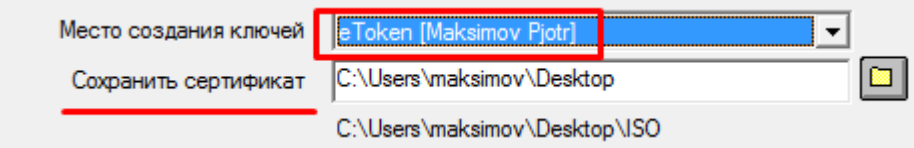

Устаналваливаем параметр «**Ключ RSA для протокола в формате ISO20022»:**



Выбираем **место создания ключей: «eTocken»** при налчии**,** либо «**Файл**».

Если ключ создается на **eToken,** предварительно, убедитесь, что **eTocken** подключен к копьютеру.

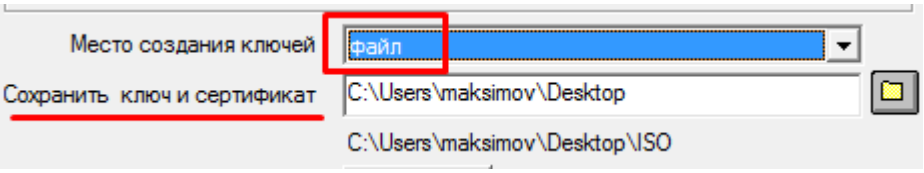
**«Сохранить сертификат»(**При генерации на **etoken):**



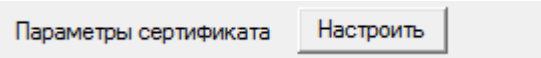

Указываем путь где будет сохранен **сертифкат ключа,** который необходимо будет выслать на аднные адреса, в архиве**:**

**maksimov@cyberplat.ru и a.titov@cyberplat.ru**

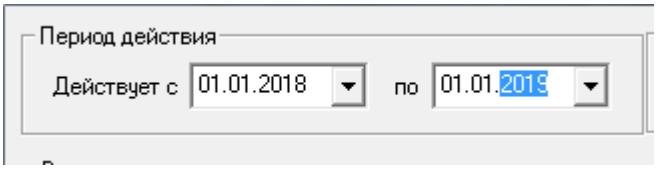
**«Сохранить ключ и сертификат»(**При генерации ключа **в «Файл»):**




Зайходим в **«Пармаетры сертификата»** нажав **«Настроить»**,




Указываем **«Период действия ключа»** один год, ровно 365 дней:




Заполняем только первый блок **«Обязательные поля».**

**Все поля заполняются строго на латинице.**

«**Населенный пункт(L)**»: указываем город, где раположен **юридический адрес организации** владельца ключа, для **юридических лиц**. Для **физических лиц** указываем город прописки.

«**Организация(O)**»: указываем наименование организации.

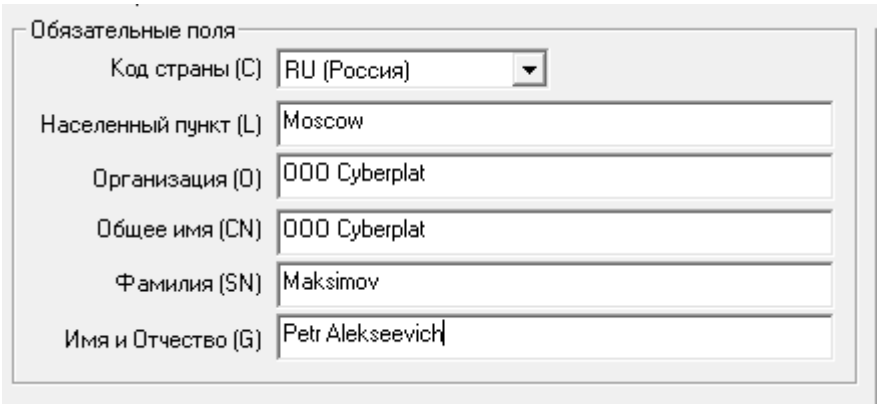
> Если **ключ** создается для **юридического лица**, указывается **наименавние организации**.
>
> Если **ключ** создается для **физического лица**, указываем **ФИО** владельца ключа, **полностью**.

«**Общее имя(CN)**»:заполняем так же как и поле «**Организация(O)».**

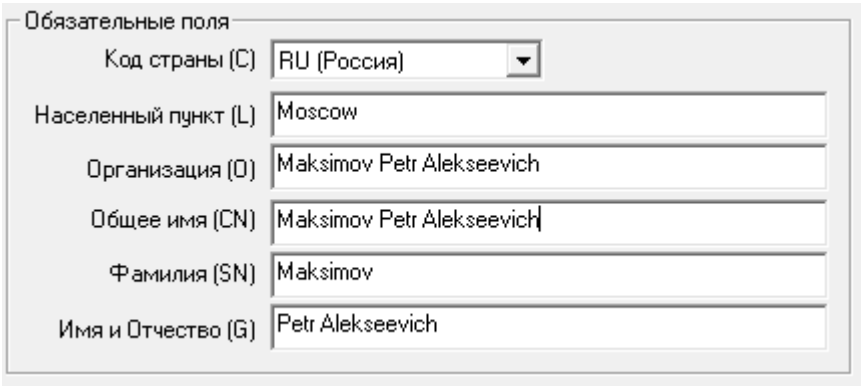
**Фамилия(SN), Имя и Отчество(G)** –указываем **ФИО** владельца ключа.

Примеры заполнения:

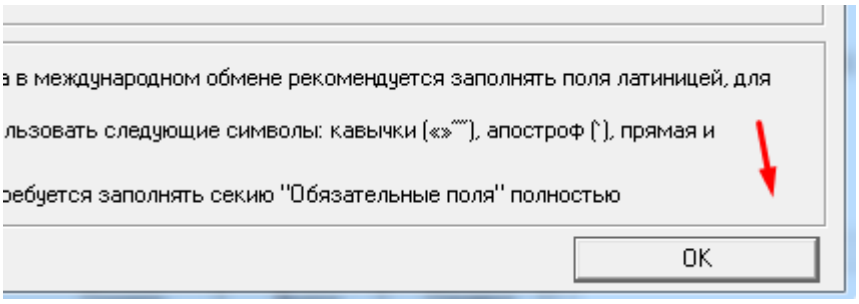
1 Юридические лицо.



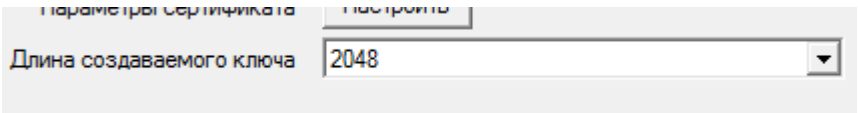

2 Физическое лицо:



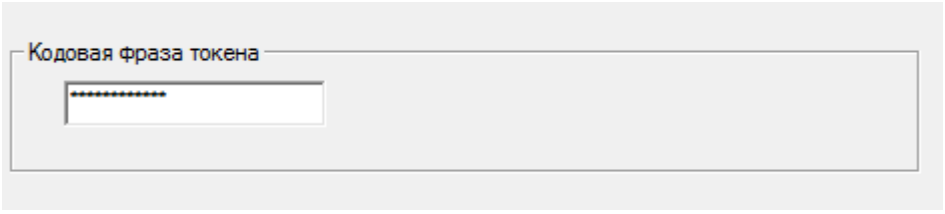

После заполнения нажимаем **«ОК»**.



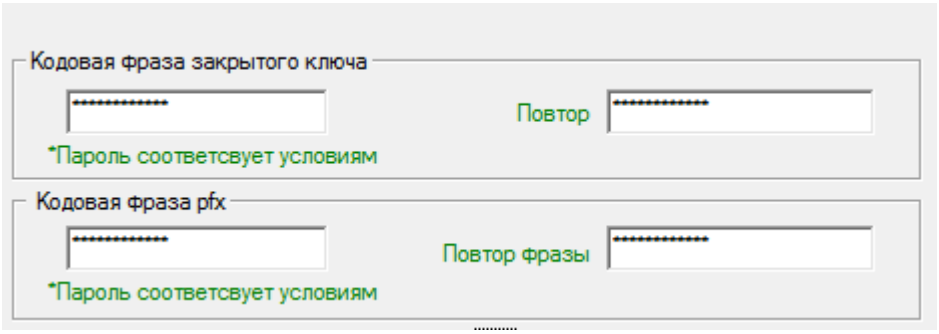

Вернувшись в предыдущее окно настроек, указываем длину создаваемого ключа **2048:**




необходимо ввести кодовую фразу от **eToken**, нажать **«создать»** при создании ключа на **eToken**:

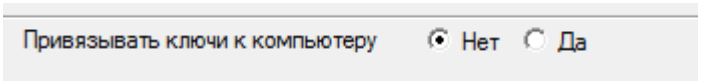



При создании ключа «**В файл**», вводим **единый пароль во все черые поля**, пароль должен быть на **латинице**, состоять из **цифр букв в вверхнем и нижнем регистре,** содержать **спец символ(!@#%)** минимум 8 символов:

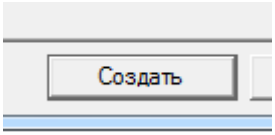



**<u>Внимание!</u> Пароль, при создании ключа в файл, необходимо обязательно запонить и сохранить. Так как в случе утраты, пароль не подлежит восстанавлению, ключ потребуется перевыпускать.**

Привязывать ключи к ompьютеру при создании **в файл** ставим нет:




Нажимаем создать:

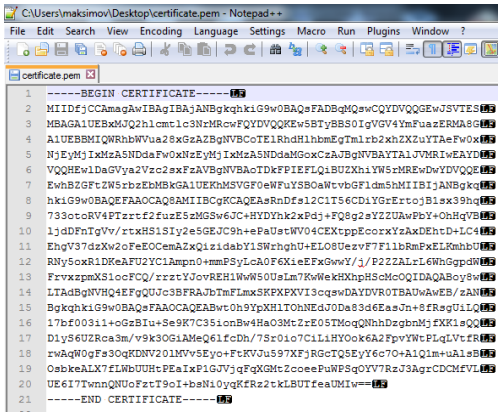



**Подготовка акта на ключ подписанта для регистрации.**

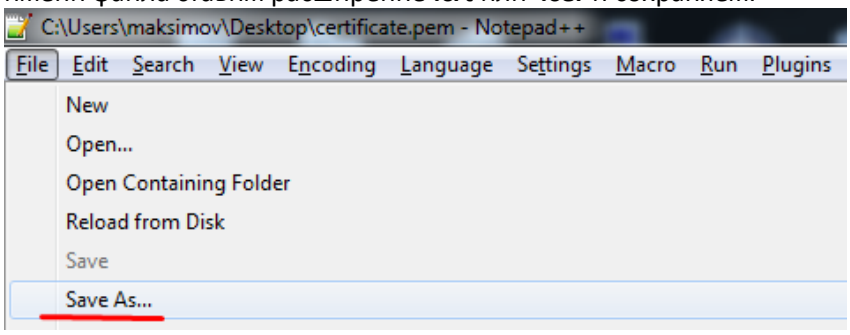
Для просмотра реквизитов сертификата через стандартное ПО для просмотра сертификатов, файл должен иметь расширение **.cer** или **.crt**.
Сертификаты подписантов, полученные в **GenKey**, обычно имеют расширение **.pem**.

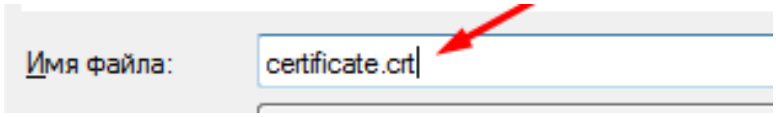
Чтобы изменить расширение, необходимо открыть файл с помощью **ПО Блокнот** или любым другим текстовым редактора.

Откроется содержание сертификата данного вида:



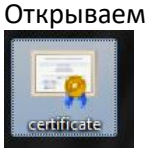

Для изменения расширения заходим в меню **«Файл»(File)**, **«Сохранить как»( Save as)**, в конце имени файла ставим расширение **.crt** или **.cer** и сохраняем.



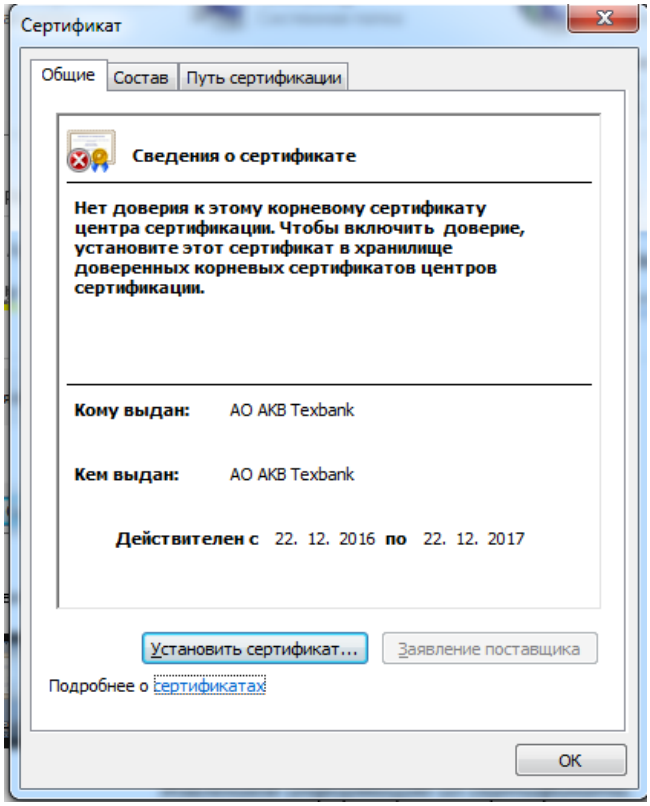




Сохраненный файл сертификата должен иметь вид:

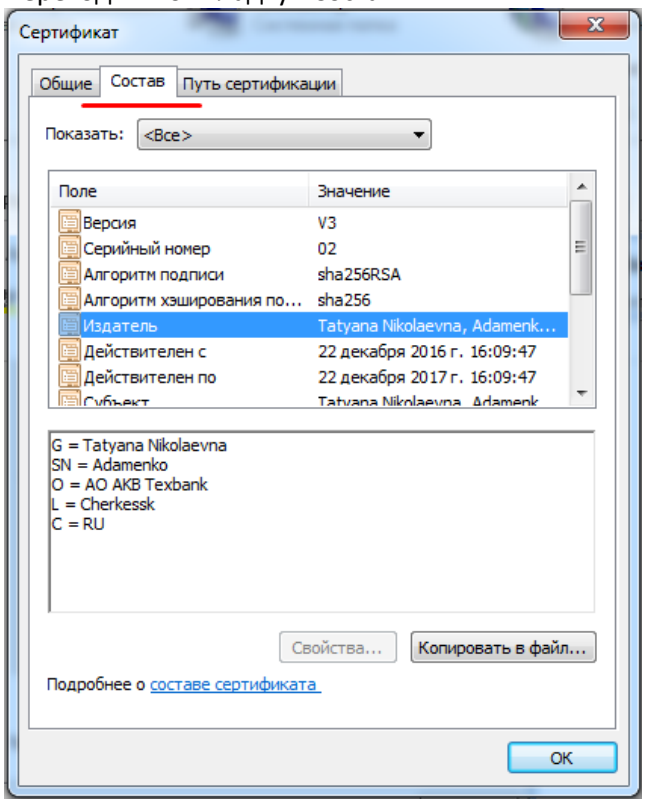

Для просмотра реквизитов сертификата откройте
Открываем изменённый файл сертификата:



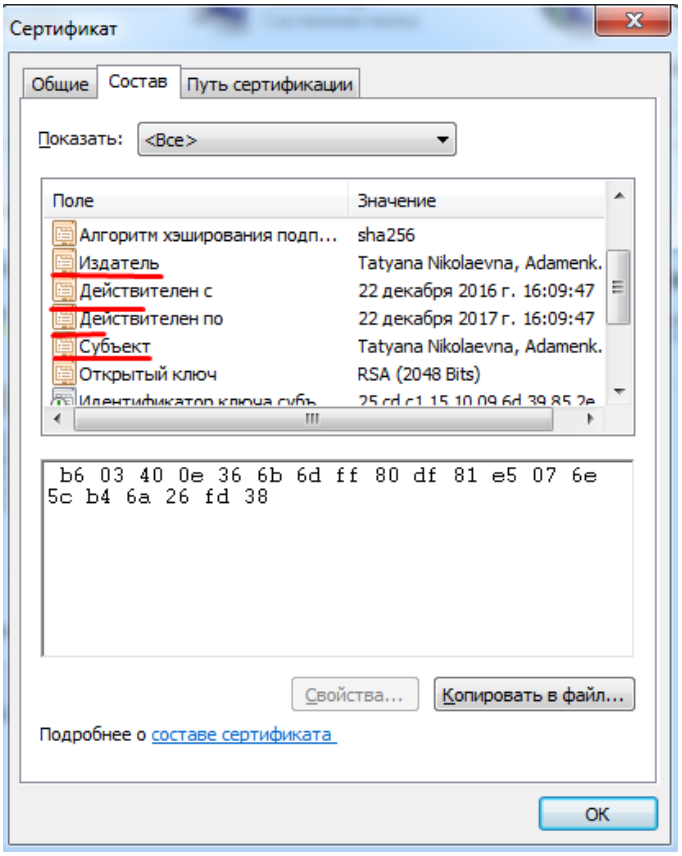

Откроется окно:

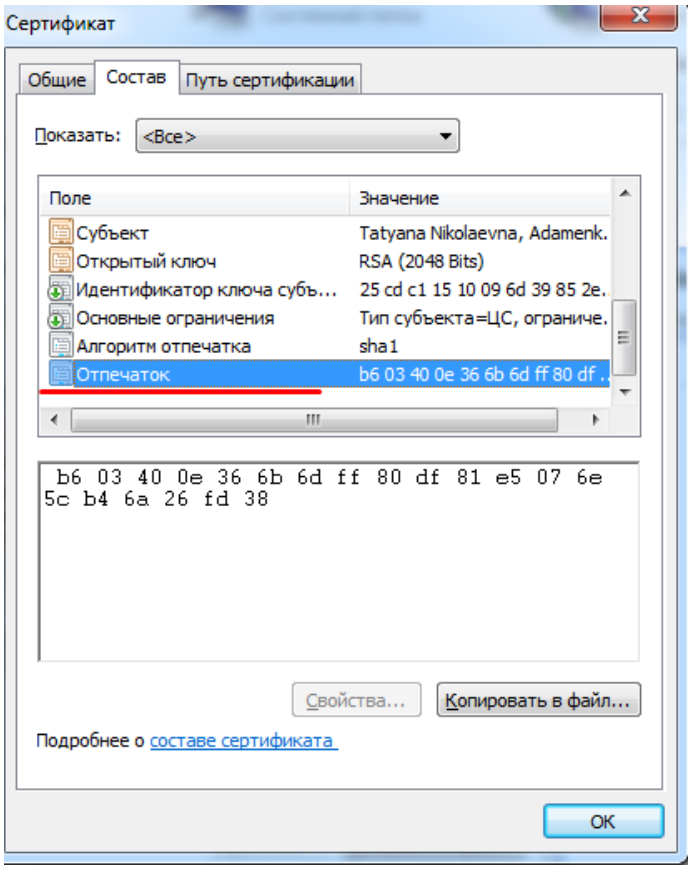



Переходим во вкладку «Состав»:




Копированием переносим в таблицу с описанием сертификата в акте, данные из параметров: **«Издатель», «Субъект», «Действителен с», «Действителен по» и «Отпечаток».**


Сертификат
Общие
Состав
Путь сертификации
Показать:
<Все>
Поле
Значение
Алгоритм хэширования подп...
sha256
Издатель
Tatyana Nikolaevna, Adamenk.
Действителен с
22 декабря 2016 г. 16:09:47
Действителен по
22 декабря 2017 г. 16:09:47
Субъект
Tatyana Nikolaevna, Adamenk.
Открытый ключ
RSA (2048 Bits)
b6 03 40 0e 36 6b 6d ff 80 df 81 e5 07 6e
5c b4 6a 26 fd 38
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK


Сертификат
Общие
Состав
Путь сертификации
Показать:
<Все>
Поле
Значение
Субъект
Tatyana Nikolaevna, Adamenk.
Открытый ключ
RSA (2048 Bits)
Идентификатор ключа субъ...
25 cd c1 15 10 09 6d 39 85 2e.
Основные ограничения
Тип субъекта=ЦС, ограниче.
Алгоритм отпечатка
sha1
Отпечаток
b6 03 40 0e 36 6b 6d ff 80 df ..
b6 03 40 0e 36 6b 6d ff 80 df 81 e5 07 6e
5c b4 6a 26 fd 38
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK

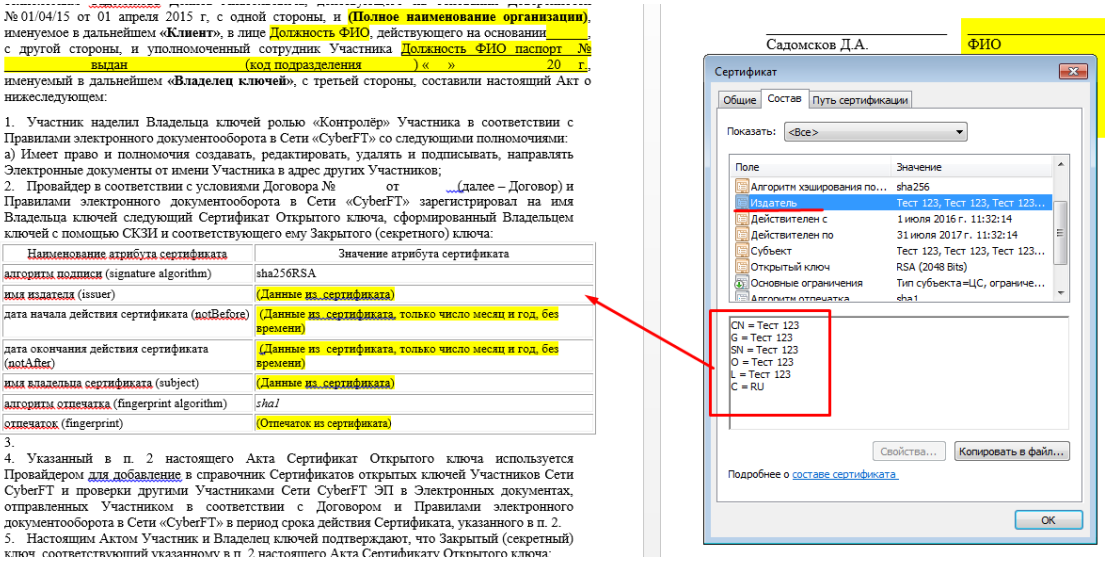
Скачиваем акт на признание ключа подписанта:

http://download.cyberft.ru/Documentation/Acts/190529%20Podpisant%20DBO.doc

**Внимание! Копируем и переносим в акт, все содержимое параметров. За исключением дат начала действия и окончания сертификата.**

**Там необходимо перенести только: число, месяц, год.**

1



№ 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:

Садомсков Д.А. ФИО

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 |

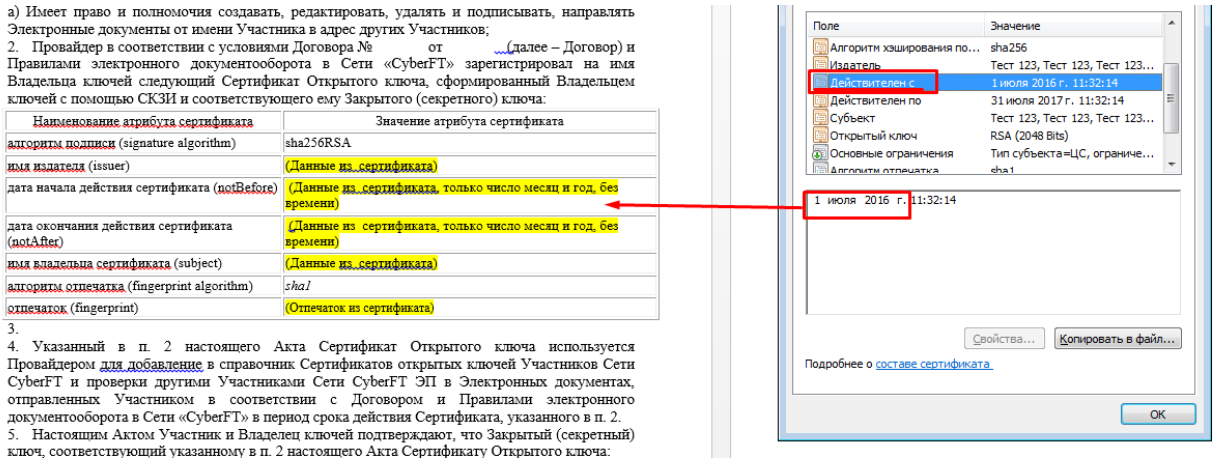
CN = Тест 123
G = Тест 123
SN = Тест 123
O = Тест 123
L = Тест 123
C = RU

Свойства… Копировать в файл…

Подробнее о составе сертификата

OK

2



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:

| 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 |

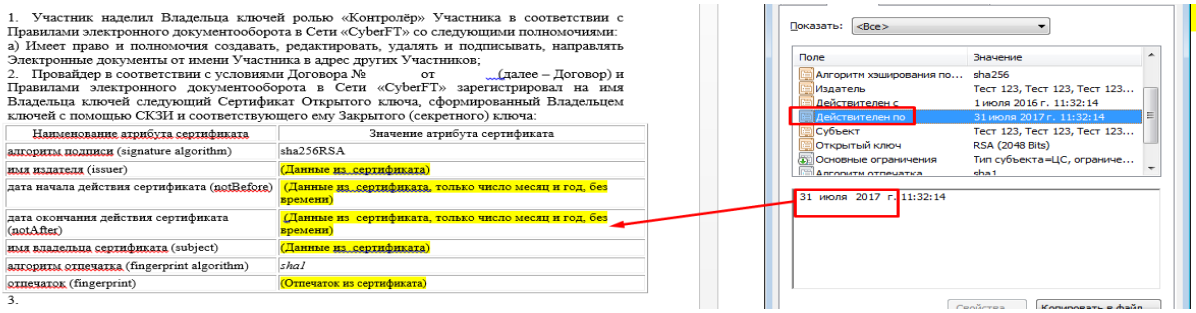
1 июля 2016 г. 11:32:14

Свойства… Копировать в файл…

Подробнее о составе сертификата

OK

3



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) |

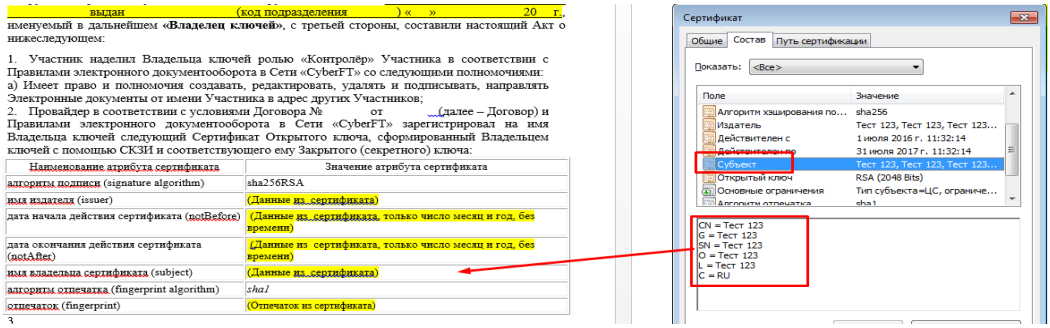
3.

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



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

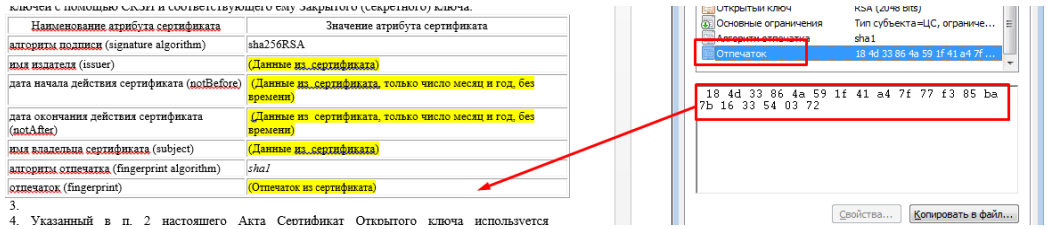
Общие | Состав | Путь сертификации

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



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

Открытый ключ RSA (2048 Bits)
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…

# Ниже пример заполнения.

# Пример заполнения таблицы в акте:

| Наименование атрибута сертификата | Значение атрибута сертификата |
|---|---|
| алгоритм подписи (signature algorithm) | sha256RSA |
| имя издателя (issuer) | CN = TEST TEST TEST.<br>O = CyberFT<br>L = Moscow<br>S = Moscow<br>C = RU |
| дата начала действия сертификата (notBefore) | 12 мая 2017 г. |
| дата окончания действия сертификата (notAfter) | 12 мая 2018 г. |

| Наименование атрибута сертификата | Значение атрибута сертификата |
|---|---|
| имя владельца сертификата (subject) | CN = TEST TEST TEST.<br>O = CyberFT<br>L = Moscow<br>S = Moscow<br>C = RU |
| алгоритм отпечатка (fingerprint algorithm) | sha1 |
| отпечаток (fingerprint) | 1 a1 a1a1 1a2a2a 22a3в3 в3в3 па5а 5а п5 |

**Внимание! Сформированный акт, в электронном виде в формате *«.doc»* и файл сертификата ключа, из которого брались данные для акта, оправить на данный адрес в архиве: cyberft@platina.ru**

**Обязательно! В теме укажите наименование вашей организации. Это поможет ускорить проверку ваших актов и сертификатов.**

# 3 Установка программы для подписания отправляемых документов.

Для подписания отправляемых документов, **обязательно** установите программу для подписания.

Скачиваете установочный файл здесь:

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

Устанавливается под администратором.

Инструкция по настройке:

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