

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.

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

Создание ключа контролёра и подготовка актов	3
Создание ключа подписанта и подготовка актов.	8
Скачивание программы GenKey	8
Установка программы для подписания отправляемых документов	17

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.

_	
Вход в систему с паролем	
··· · · · · · · · · · · · · · · · · ·	
Email	
	1
admin@cyberft.com	
	,
Пароль	
]
••••••	J
Войти в систему	

Потребуется установка нового пароля:

брос пароля	
Старый пароль	предоставленный ранее пароль.
Новый пароль	новый пароль
Подтверждение пароля	повто нового пароля
Сохранить	

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»:

¢	Настройки	
	Общие	
	Терминалы	

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

Недоступен	Настройки	-
	· · · · · · · · · · · · · · · · · · ·	

Выбираем вкладку «Ключи контролёра» далее нажимаем создать ключ:

Управление обя	иеном Ключи конт	тролера Настройк	и подлисания Наст	пройки автоматического	подлисания	Пользователи
Connath street	Autoontunosami attoo	-	_			
-	Наименование	References and and				

Выбираем ID необходимого вам терминала.

«Первичный или дополнительный ключ» ставим «Первичный».					
Первичный или дополнительный ключ	BKSERUM@AMLT (OOO "5KC")				
		٩			
ID Терминала	BKSERUM@AMLT (OOO "6KC")	*			

Первичный или дополнительный Первичный ключ 🔹

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

ключ

Личный ключ/Ключ организации

Ключ организации

Далее заполняем реквизиты.

v

 Реквизиты сертификата	
 Фамилия владельца ключа (SN)	Ivanov
 Owner name (G)	Ivan Ivanovich
 Наименование организации (О)	Best Company, LLC
 Страна (С)	RU
Область или провинция (S)	Moscow
Населенный пункт (L)	Moscow
Пароль	

Далее вводим и подтверждаем пароль.

<u>Обязательно!</u> Запомните и по возможности сохраните\запишите данный пароль. Он потребуется для запуска терминала. Данный пароль, восстановлению не подлежит.

<u>Внимание!</u> Не передвайте данный пароль третьим лицам и сторонним организациям, во избежание его попдания в руки злоумышлинников.

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.

Активация ключа контр	оолера 🛛 🗙
Пароль ключа:	
	Активировать

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

Ключ ус	пешно активирован
Назад	Деактивировать
Параме	етры ключа

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:

Файлы ключа



1.4. Подготовка акта признания.

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

Сформировать акт о признании ЭП

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»

ип договора		Номер договора	Дата договора
Выберите тип		•	iii ×
Уполномоченный предста	авитель клиента		
з лице: ФИО полностью			
Иванова Ивана Ивановича			
Занимающего должность			
Генерального директора			
јействует на основании			
Владелец ключа			
ФИО полностью			
Олжность			
_			
аспортные данные влад	цельца ключа		
Страна выдачи	Серия	Номер	Код подразделения
PΦ			
бем выдан			Дата выдачи
			i ×

<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: <u>cyberft@platina.ru</u>

<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»:

Создание ключей Импорт открытых ключей Ключи на е Toker	Настройки	
Страна Россия ТЕСТ		
Карточка ключа		

Устанавлвиваем парметр «Использовать расширенный режим интерфейса»:

- тепересете кодобло трабу и путе к каке какта отраницу инперта к —
- Импортировать необходимые открытые ключи после генерации кли
- Использовать расширенный режим интерфейса программы
- Использовать прокси

11-----

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»:

Ключ RSA для протокола	в Формате ISO20022	
Место создания ключей		-

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):

Место создания ключей	eToken [Maksimov Pjotr]	-	
Сохранить сертификат	C:\Users\maksimov\Deskto	p	
	C:\Users\maksimov\Deskto	p\ISO	

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

<u>maksimov@cyberplat.ru</u> и <u>a.titov@cyberplat.ru</u>

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

Место создания ключей	Файл	
Сохранить ключ и сертификат	C:\Users\maksimov\Desktop	
	C:\Users\maksimov\Desktop\ISO	

Зайходим в «Пармаетры сертификата» нажав «Настроить»,

Параметры сертификата Настроить

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

Период действ	зия			
Действует с	01.01.2018	•	по 01.01. <mark>2019</mark>	-

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(О)»: 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(О)».

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

Примеры заполнения:

1 Юридические лицо.

— Обязательные поля— Код страны (С)	RU (Россия)
Населенный пункт (L)	Moscow
Организация (О)	000 Cyberplat
Общее имя (CN)	000 Cyberplat
Фамилия (SN)	Maksimov
Имя и Отчество (G)	Petr Alekseevich

2 Физическое лицо:

Обязательные поля	
Код страны (С)	RU (Россия)
Населенный пункт (L)	Moscow
Организация (О)	Maksimov Petr Alekseevich
Общее имя (CN)	Maksimov Petr Alekseevich
Фамилия (SN)	Maksimov
Имя и Отчество (G)	Petr Alekseevich

После заполнения нажимаем «ОК».

а в международном обмене рекомендуется заполнят	ъ поля латиницей, для
льзовать следующие символы: кавычки («» […]), апост	роф (`), прямая и
ребуется заполнять секию "Обязательные поля" пол	ностью
	ОК

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

параметры сертификата	построято
Длина создаваемого ключа	2048

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

Кодовая фраза токена	

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:

Кодовая фраза закрытого ключа	а Повтор м	
Кодовая Фраза pfx	Повтор фразы м	

<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.

<u>Внимание!</u> Не передавайте данный пароль тртьим лицам и сторонним организациям, во избежание компрометации ключа и попдания в руки злоумышлинников.

Привязывать ключи к омпьютеру при создании в файл ставим нет:

Привязывать ключи к компьютеру	€ Нет	С Да
Нажимаем создать:		
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:

C:\0	sers(maksimov)Desktop)certificate.pem - Notepad++
File E	dit Search View Encoding Language Settings Macro Run Plugins Window ?
6) = e 6 6 8 4 % h h > c # ½ * * E 5 = TIBC 🛽
😑 certif	icate.pem 🖾
1	BEGIN CERTIFICATE
2	MIIDfjCCAmagAwIBAgIBAjANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJSVTES
3	MBAGA1UEBxMJQ2hlcmtlc3NrMRcwFQYDVQQKEw5BTyBBS0IgVGV4YmFuazERMA8G
4	A1UEBBMIQWRhbWVua28xGzAZBgNVBCoTE1RhdH1hbmEgTm1rb2xhZXZuYTAeFw0x
5	NjEyMjIxMzA5NDdaFw0xNzEyMjIxMzA5NDdaMGoxCzAJBgNVBAYTA1JVMRIwEAYD
6	VQQHEw1DaGVya2Vzc2sxFzAVBgNVBAoTDkFPIEFLQiBUZXhiYW5rMREwDwYDVQQE
7	EwhBZGFt2W5rbzEbMBkGA1UEKhMSVGF0eWFuYSBOaWtvbGF1dm5hMIIBIjANBgkq
8	hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsRnDfsl2C1T56CDiYGrErtojB1sx39hq
9	733otoRV4PTzrtf2fuzE5zMGSw6JC+HYDYhk2xPdj+FQ8g2sYZZUAwPbY+OhHqVB
10	ljdDFnTgVv/rtxHS1SIy2e5GEJC9h+ePaUstWV04CEXtppEcorxYzAxDEhtD+LC4
11	EhgV37dzXw2oFeEOCemAZxQizidabY1SWrhghU+ELO8UezvF7F11bRmPxELKmhbU
12	RNy5oxR1DKeAFU2YC1Ampn0+mmPSyLcA0F6XieEFxGwwY/j/P2ZZALrL6WhGgpdW
13	FrvxzpmXSlocFCQ/rrztYJovREH1WwW50UsLm7KwWekHXhpHScMcOQIDAQABoy8w
14	LTAdBgNVHQ4EFgQUJc3BFRAJbTmFLmxSKPXPXVI3cqswDAYDVR0TBAUwAwEB/zAN
15	BgkqhkiG9w0BAQsFAAOCAQEABwt0h9YpXH1TOhNEdJ0Da83d6EasJn+8fRsgUiLQ
16	17bf003i1+oGzBIu+Se9K7C35ionBw4HaO3MtZrE05TMogQNhhDzgbnMjfXK1sQQ
17	D1yS6UZRca3m/v9k30GiAMeQ61fcDh/7Sr0io7CiLiHYOok6A2FpvYWtPLqLVtfR
18	rwAqW0gFs30qKDNV201MVv5Eyo+FtKVJu597XFjRGcTQ5EyY6c70+A1Q1m+uA1sB
19	OsbkeALX7fLWbUUHtPEaIxP1GJVjqFqXGMtZcoeePuWPSqOYV7RzJ3AgrCDCMfVL
20	UE617TwnnQNUoFztT9oI+bsNi0yqKfRz2tkLBUTfeaUMIw==
21	END CERTIFICATE

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

C:\Users\maksimov\Desktop\certificate.pem - Notepad++									
<u>F</u> ile	e <u>E</u> dit	<u>S</u> earch	<u>V</u> iew	E <u>n</u> coding	<u>L</u> anguage	Se <u>t</u> tings	<u>M</u> acro	<u>R</u> un	<u>P</u> lugins
	New								
	Open								
	Open Containing Folder								
	Reloa	d from Di	sk						
	Save								
	Save /	4s							
			_						
Имя файла: certificate.crt									

Сохраненный файл сертификата должен иметь вид:



Для просмотра реквизитов сертификата откройте Открываем изменённый файл сертификата:



Откроется окно:

Сертификат	
Общие Состав Путь сертификации	1
Сведения о сертификате	
Нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации.	
Кому выдан: AO AKB Texbank	
Кем выдан: AO AKB Texbank	
Действителен с 22. 12. 2016 по 22. 12. 2017	
Установить сертификат Заявление поставщика Подробнее о сертификатах	
ОК)

Переходим во вкладку «Состав»:

Сертификат	×
Общие Состав Путь сертифика	ции
Показать: <Все>	▼
Поле	Значение
Версия Серийный номер	V3 02 ≡
Алгорити хэширования по	sha256
🗒 Издатель	Tatyana Nikolaevna, Adamenk
Действителен с Действителен по	22 декабря 2016 г. 16:09:47 22 декабря 2017 г. 16:09:47
	Tatvana Nikolaevna Adamenk
G = Tatyana Nikolaevna SN = Adamenko O = AO AKB Texbank L = Cherkessk C = RU	
Се Подробнее о <u>составе сертификат</u>	юйства Копировать в файл а_
	ОК

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	1
<u>П</u> оказать: 	•
Поле	Значение
Алгоритм хэширования подп Издатель Действителен с Действителен по Субъект Открытый ключ	sha256 Tatyana Nikolaevna, Adamenk. 22 декабря 2016 г. 16:09:47 22 декабря 2017 г. 16:09:47 Tatyana Nikolaevna, Adamenk. RSA (2048 Bits) 25 cd c1 15 10 09 6d 39 85 2e
b6 03 40 0e 36 6b 6d f 5c b4 6a 26 fd 38	f 80 df 81 e5 07 6e
Свой Подробнее о <u>составе сертификата</u>	тва Копировать в файл
	ОК

ертификат		x
Общие Состав Путь сертификаци	и	
<u>П</u> оказать: 	•	
Поле	Значение	*
Субъект Открытый ключ Идентификатор ключа субъ Основные ограничения Алгоритм отпечатка	Tatyana Nikolaevna, Adamenk. RSA (2048 Bits) 25 cd c1 15 10 09 6d 39 85 2e. Тип субъекта=ЦС, ограниче. sha1	III
🔲 Отпечаток	b6 03 40 0e 36 6b 6d ff 80 df	-
•	•	
b6 03 40 0e 36 6b 6d f 5c b4 6a 26 fd 38	f 80 df 81 e5 07 6e	
, <u>Свой</u> Подробнее о <u>составе сертификата</u>	іства Копировать в файл	
		(

1

2

3

Скачиваем акт на признание ключа подписанта:

http://download.cyberft.ru/Documentation/Acts/190529%20Podpisant%20DB O.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., о именуемое в дальнейшем «Клиент» с другой стороны, и уполномоче выдая именуемый в дальнейшем «Владел именуемый в дальнейшем «Владел именуемый в дальнейшем «Владел именет правилами электронного документо а) Имеет право и полномочия созд Электронные документы от имени У 2. Провайдер в соответствии с усло Правилами электронного докумен Владелыца ключей следующий Сер ключей с помощьо СКЗИ и соответс Навленсование атрябута сертификат	с одной стороны, и (Полное наименование организации) в лице Должность ФИО, действующего на основания ный согрудник Участника Должность ФИО паспорт М (код подразделения) « » 20 г. ец ключей», с третьей стороны, составили настоящий Акт с спочей ролью «Контролёр» Участника в соответствии с оборота в Сети «СубенГГ» со следующими полномочиями: завть редактировать, удалять и подписквать, направлять частника в адрес других Участников; виями Договора № от (далее – Договор) и тооборота в Сети «СубенГГ» зарегистрировал на имя тификат Открытого ключа, сформированный Владельцем тирующего ему Закрытого (скретного) ключа: а Зичение атрибута сертификата	Cept Of	ФНО ФНО К ФНО К ФНО К К ФНО К К ФНО К К К К К К К К К К К К К	
алгоритм подписи (signature algorithm)	sha256RSA		Открытый ключ RSA (:	2048 Bits)
имя издателя (issuer)	(Данные из сертификата)		Основные ограничения Тип су	/бъекта=ЦС, ограниче 👻
дата начала действия сертификата (<u>notB</u>	efore) (Данные из сертификата, только число месяц и год, без времени)		N = Tect 123	
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)		N = Tect 123 = Tect 123 = Tect 123	
имя владельца сертификата (subject)	(Данные из сертификата)	č	= RU	
алгориты отпечатка (fingerprint algorithm	a) shal			
отнечаток (fingerprint) 3. 4. Указанный в п. 2 настоящего Акта Сертификат Открытого ключа используется Провайдером для добавление в справочник Сертификатов открытых ключей Участников Сети СуberFT и проверки другими Участниками Сети СуberFT ЭП в Электронных сокументах, отправленных Участников с соответствии с Договором и Правилами электронныго документооборота в Сети «СуberFT» в период срока действия Сертификата, указанного в п. 2. 5. Носолятис Алгом Участни В взараем стояма докуметалор по Заличитий (саковати й)			Свойства дробнее о <u>составе сертификата.</u>	Копировать в файл ОК
ключ соответствующий указанному 2 а) Имеет право и полномочия создавать Электронные документы от имени Участн	в п 2 настоящего Акта Сертивикату Открытого ключа: , редактировать, удалять и подписывать, направлять ика в адрес других Участников;		None	Значение
 Провайдер в соответствии с условиям Правилами электронного документообо Владельца ключей следующий Сертифии ключей с помощью СКЗИ и соответствую 	и Договора № от(далее – Договор) и рота в Сети «СуренFТ» зарегистрировал на имя кат Открытого ключа, сформированный Владельцем шего ему Закрытого (секретного) ключа:	-1	Алгоритм хэширования по Издатель Аействителен с	sha256 Тест 123, Тест 123, Тест 123. 1 июля 2016 г. 11:32:14 31 июля 2017 г. 11:32:14
Наименование атрибута сертификата	Значение атрибута сертификата		Субъект	Тест 123, Тест 123, Тест 123.
алгоритм подписи (signature algorithm)	sha256RSA		Основные ограничения	ком (2046 bits) Тип субъекта=IIC, ограниче
имя издателя (issuer)	(Данные из_сертификата)			cha1
дата начала действия сертификата (<u>notBefore</u>)	(Данные из. сертификата, только число месяц и год, без времени)		1 июля 2016 г. <mark>11:32:14</mark>	

дата начала действия сертификата (<u>notBefore</u>)	(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)
има владельца сертификата (subject)	(Данные из_сертификата)
алгорнтм отпечатка (fingerprint algorithm)	shal
ornewarok (fingerprint)	(Отпечаток из сертификата)
3.	

Указанный в п. 2 настоящего Акта Сертификат Открытого ключа используется Провайдером <u>для добавление</u> в справочник Сертификатов открытых ключей Участников Сети СуberFT и проверки другими Участниками Сети СуberFT ЭП в Электронных документах, опправленных Участником в соответствии с Договором и Правилами электронного документооборога В Сети «СуberFT» 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:

<u>С</u>войства... <u>Копировать в файл...</u>

ОК

ее о составе серт

фиката

ООО «КИБЕРПЛАТ»

Участник наделил Владельца ключе завилами электронного документооборо Имеет право и полномочия создавать тектронные документы от имени Участн Провайдер в соответствии с условиям завилами электронного документообс адаелыд ключей с лемующью СКЗИ и соответствую	й ролью «Контролёр» Участника в соответствии с та в Сети «СуberFT» со следующими полномочими: редактировать, удалять и подписывать, направлять ика в адрес других Участников; и договора № отдалее – Договор) и рота в Сети «СуberFT» зарегистрировал на имя кат Открытого ключа, сформированный Владельцем щего ему Закрытого (скрентного) ключа:		азать: < <u>Все></u> Алгоритн хэширования по Издатель Лействителен с Действителен по	Эначение sha256 Тест 123, Тест 123, Те 1июля 2016 г. 11:32: 31июля 2017 г. 11:32
Наименование атрибута сертификата	Значение атрибута сертификата		Субъект	Тест 123, Тест 123, Те
алгоритм подписи (signature algorithm)	sha256RSA		Открытый ключ	RSA (2048 Bits)
имя издателя (issuer)	(Данные из сертификата)		Алгорити отпечатка	cha1
дата начала действия сертификата (<u>notBefore</u>)	(Данные <u>из. сертификата,</u> только число месяц и год, без времени)	31	июля 2017 г. 11:32:14	
дата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)			
имя владельца сертификата (subject)	(Данные из сертификата)			
алгориты отпечатка (fingerprint algorithm)	shal			
отпечаток (fingerprint)	(Отпечаток из сертификата)			
3.				Konunne

4

выдан (к	20			
	од подразделения) « » 20 г.,	Сертиф	фикат	
именуемый в дальнейшем «владелец клі нижеследующем:	ючен», с третьен стороны, составили настоящий Акт о	Общи	е Состав Путь сертифика	ации
 Участник наделил Владельца ключей 	й ролью «Контролёр» Участника в соответствии с			
Правилами электронного документооборо	та в Сети «CyberFT» со следующими полномочиями:	Цока	зать: <bce></bce>	•
 а) Имеет право и полномочия создавать, 	редактировать, удалять и подписывать, направлять			
Электронные документы от имени Участн	ика в адрес других Участников;	1107	ne	значение
 Провандер в соответствии с условиями Полицирании ответствии с условиями 	I Dorobopa No or (danee – Dorobop) H		Алгоритм хэширования по	sha256
правилали электронного документосоор Владельца ключей спетующий Сертифия	ат Открытого ключа сформированный Владельнем		Издатель Лайствитален с	1 word 2016 r 11:32:14
ключей с помошью СКЗИ и соответствую	шего ему Закрытого (секретного) ключа:		Дейстрителен по	31 июля 2017 г. 11:32:14
Наименование атрибута сертификата	Значение атрибута сертификата		Субъект	Тест 123, Тест 123, Тест 123
агоритм подписи (signature algorithm)	sha256RSA		Открытый ключ	RSA (2048 Bits)
иля издателя (issuer)	(Данные из_сертификата)		Авгорити отпецатка	cha1
дата начала действия сертификата (<u>notBefore</u>)	(Данные из <u>сертификата,</u> только число месяц и год, без времени)	CN =	= Tect 123	
цата окончания действия сертификата (notAfter)	(Данные из сертификата, только число месяц и год, без времени)	SN = 0 =	- Тест 123 Тест 123	
имя владельца сертификата (subject)	(Данные из_серлификата)	L = C =	RU IZ3	
агориты отпечатка (fingerprint algorithm)	shal			
THENATOR (fingerprint)				
3	(отпечаток из сертификата)		_	
5 5	Uniteritor ito ceptiepitatai			KSA (2048 BITS)
5 Ключен с полощью Скълт и соответствук Наименование атрибута сертификата	(Оппечнок на серпериата) лцего свлу Закувытого (текретилого) ключа. Значение агрибута сертификата		Открытыи ключ Основные ограничения	къя (дича вла) Тип субъекта=ЦС, ограниче
КЛОЧЕН С ПОМОЩЬЮ СКЪРГ И СООТВЕТСТВУК Наименование агрибута сергификата алсориты подщека (signature algorithm)	онненток во серпералата) лицен о ему закуваном о (секретаном о) влаоча. Зпачение атрибута сертификата sha256RSA		Открытыи ключ Основные ограничения Акторити открыти	Кък (дина ЫТБ) Тип субъекта=ЦС, ограниче sha 1 18 del 316 da 150 1 баl 1 ad 77
Какчен с помощью сколт и соответствук Наполенование атрибута сертификата апториты подлики (signature algorithm) имя взаятая (issuer)	оппечнок во серпериата) лијсто слау Закуватото (псекретичкот и клютка. Значение агрибута сертификата (Данные из сертификата)		Открытыи ключ Основные ограничения Ангорити открытися Отпечаток	къл ("оча ыт.5) Тип субъекта=ЦС, ограниче sha1 18 4d 33 86 4a 59 1f 41 a4 7f
Ключен с полощью слуги и соответствук Наконование атрибута сертификата алгориты полики (signature algorithm) имя издателя (issuer) дата начала действия сертификата (<u>notBefore</u>)	оппеннов на серпериата) лисето силу закуватото (сседетляло од клюма. Значение атрибута серпефиката sha256RSA (Даниме из серпефиката) (Даниме из серпефиката) гДаниме из серпефиката топко число месяц и год, без времени)		UTROPETEM КЛЮЧ Основные ограничения Ангрити отпочения Стлематок 14 - 23 26 4а 59 11 14 - 23 26 4а 59 11	KSA (JUND BIG) Tim cyfsecta=UC, orpanne dha1 18 ed 33 86 48 59 1f 41 a4 7f f 41 a4 7f 77 f 3 85 ba
Ключен с полющью скъзт и соответствук Напоснование агрибута сертификата апториты полинея (signature algorithm) изя изадляетя (issuer) дата начала действия сертификата (notBefore) дата окончания действия сертификата (notAfter)	оппентов из сертификата) лицен о силу Закранного (секретняло ор клюоча. Зпачение атрибута сертификата им.256RSA (Данные из сертификата, топько число месяц и год, без врамения) (Данные из сертификата, топько число месяц и год, без врамения)		Uпсрытын ключ Основные огранчения Агерити колочать Оптечаток 8 4d 33 86 4а 59 11 16 33 54 03 72	към ("чер воду Тип субъекта=ЦС, ограниче dha1 18 41 33 6 48 59 17 41 ан 77 f 41 а.4 7 f 77 f 3 85 ba
Ключен с помощью скъзг и соответствук Наименование атрибута сертификата алгориты полники (signature algorithm) имя издателя (issuer) дата начала действия сертификата (поШебле) гата осногнания действия сертификата (поАйдея) имя взадельна сертификата (subject)	оппечнок из сергнариата) листо с клу Закуваного (секрствого) ключа. Значение агрибута сергнафиката sha256RSA (Данные из сергнафиката) (Данные из сергнафиката, топько число месяц и год, без времени) (Данные из сергнафиката)	1 7b	ипрытын ключ Соювные отраничения Леорини этраничения Отпечаток 8 4d 33 86 4a 59 11 16 33 54 03 72	KSA (2049 815)) In cyfoberta=UC, orpanse shal 18 45 33 66 48 59 1f 41 64 7f f 41 a4 7f 77 f3 85 ba
Ключен с полющью слуги и соответствук Наяменование атрябута сертификата акториты полице (signature algorithm) имя издителя (signature algorithm) дата начала действия сертификата (подАйс) илата окончания действия сертификата (подайс) ила владелица сертификата (subject) акториты стивчата, (fingerprint algorithm)	сипеннов на сертификата) лицего сиху Закуваного (пекретного) ключа. Значение агрибута сертификата sha256RSA (Данные из. сертификата, топько число месяц и год, без премения) (Данные из. сертификата) sha1		Uпорытын клоч Основные отраничения Асерина эток цати Оплечаток 8 4d 33 86 4a 59 11 16 33 54 03 72	нска (диче вск5) Тип субеста=ЦС, ограниче яна 18 на 33 86 на 59 1 f a1 a4 7 f f 41 a4 7 f 77 f 3 85 ba
Ключен с помощью склят и соответствук Навыевование атрибула сертификата авториты подписи (signature algorithm) имя издателя (issuer) дата начала действия сертификата (доШебоце) дата окончания действия сертификата (досАйес) имя властная сертификата (subject) авториты отпечата; (fingerprint algorithm) отпечанах; (fingerprint)	ицето силу закрытото (севретияного) влютча. Значение агрибута сертификата sha256RSA (Данные из сертификата) (Данные из сертификата, только число месяц и год, без времени) (Данные из сертификата, только число месяц и год, без времени) (Данные из сертификата) sha1 (Ситечнок из сертификата)		ипфитын ключ Основные огранчения Анерипи саранчения Слемато: 16 33 54 03 72	към (диео воя) Тип субъекта=ЦС, ограниче sha1 18:4d 3386:4b 59 1f 41 a4 7f f 41 a4 7f 77 f3 85 ba
Ключен с полющью СК.574 и СООзветствук Наименование атрибула сертификата алсориза поликев (signature algorithm) има издателя (sisuer) дата изчала действия сертификата (nollefore) дата окончания действия сертификата (nolAfter) има владельна сертификата (subject) алсориза силезатка (fingerprint algorithm) отпечаток (fingerprint) 3.	оппечнок из серпералата) лицен о сму Закранного (сседетняло ор клюоча. Значение атрибута сертификата sha256RSA (Данные из сертификата) (Данные из сертификата, топько число месяц и год, без времени) (Данные из сертификата, топько число месяц и год, без времени) (Данные из сертификата) (Данные из сертификата) (Данные из сертификата)	in the second se	Uпкрытын клоч Основные огранчения Агеррин алгана Оленаток 16 33 54 03 72 1	към ("UMB DIG) Тип субъекта=ЦС, ограниче dba1 19 4d 33 86 45 59 1f 41 a4 7f f 41 a4 7f 77 f 3 85 ba робстир

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. O = CyberFT L = Moscow S = Moscow 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. O = CyberFT L = Moscow S = Moscow C = RU
алгоритм отпечатка (fingerprint algorithm)	sha1
отпечаток (fingerprint)	1 а1 а1а1 1а2а2а 22а3в3 в3в3 па5а 5а п5

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

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

<u>Внимание!</u> Передать необходимо только *certificate.pem* или *certificate.crt*. Откуда были взяты данные для акта. Файлы *certificate.pfx* и *private_key.key* **должны находится только у вас.** Не передавайте данные файлы третьим лицам и сторонним организациям во избежание компрометации и попадания ключа в руки злоумышленников.

Если вы передадите для регистрации *certificate.pfx* или *private_key.key* мы не сможем принять данный ключ в работу, так как он будет скомпрометирован. Потребуется повторное создание ключа.

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