Утверждаю:
Директор
Закрытого акционерного общества «Центр Цифровых Сертификатов»

_____ А. Ю. Леонов

«01» августа 2016 г.

ПРАВИЛА РАБОТЫ ЦЕНТРА ЦИФРОВЫХ СЕРТИФИКАТОВ «BESAFE.RU»

Правила вступают в силу с 01 августа 2016г.

1. Введение

1.1. Термины и определения

Агент ЦЦС «BESAFE.RU» (Агент) - уполномоченный представитель ЦЦС, которому ЦЦС доверил выполнение операций по идентификации, аутентификации при изготовлении Сертификатов, проверке полномочий Владельцев сертификатов (ЦЦС делегирует Агенту часть своих полномочий) и передаче сформированных ими Запросов сертификатов Администратору ЦЦС, но не имеющий полномочий на подписание и выпуск Сертификатов. Обладает необходимым комплексом программно-технических средств ЭП и шифрования для организации защищенного канала связи, обеспечивающего достоверную передачу Запросов сертификатов Владельцев сертификатов в ЦЦС.

На усмотрение ЦЦС, ЦЦС может исполнять часть либо все обязанности Агента.

Администратор ЦЦС «BeSafe.ru» - уполномоченное лицо ЦЦС, ответственное за выполнение операций по регистрации Владельцев сертификатов, изготовлению и обслуживанию Сертификатов Владельцев сертификатов, заверению Списков отозванных сертификатов. Возможно частичное делегирование полномочий Администратора лицам, уполномоченным ЦЦС.

Аутентификация Владельца сертификата – процедура проверки принадлежности заявленного идентификатора Владельцу сертификата (субъекту идентификации).

Владелец сертификата ключа проверки ЭП (Владелец сертификата) – физическое лицо или юридическое лицо в лице уполномоченного представителя, на имя которого ЦЦС выдан Сертификат ключа проверки ЭП, и которое владеет соответствующим Ключом ЭП, позволяющим с помощью Средств ЭП создавать свою ЭП в электронных документах (подписывать электронные документы).

Запрос сертификата - электронный документ, содержащий Ключ проверки ЭП и сведения о Владельце сертификата, заверенные его ЭП.

Защищенный сервис – системы защищенного взаимодействия на базе PKI, имеющие различное прикладное назначение.

Идентификация Владельца сертификата – процедура, направленная на определение идентификатора, однозначно соответствующего Владельцу сертификата (субъекту идентификации), где идентификатор – это уникальный набор значений признаков (для физических лиц - фамилия, имя, отчество; для юридических лиц - наименование, ФИО представителя, адрес местонахождения и ОГРН; а также прочие признаки, например, паспортные данные), однозначно отличающий одного Владельца сертификата от других.

Инфраструктура открытых ключей (Public Key Infrastructure - PKI) - интегрированный набор служб и средств администрирования для создания и развертывания приложений, использующих криптографию с Ключами проверки ЭП; обеспечивает функции управления Ключами проверки ЭП.

Квалифицированный сертификат ключа проверки ЭП (Квалифицированный сертификат) - Сертификат ключа проверки ЭП, выданный аккредитованным Удостоверяющим центром или доверенным лицом аккредитованного Удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП (уполномоченный федеральный орган).

Ключ ЭП (Закрытый ключ, Секретный ключ, Ключ) – уникальная последовательность символов, известная Владельцу сертификата и предназначенная для создания ЭП.

Ключ проверки ЭП (Открытый ключ) - уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП (далее – «проверка ЭП»).

Компрометация ключа – констатация Владельцем сертификата обстоятельств, при которых возможно несанкционированное использование его Ключа ЭП неуполномоченными лицами.

Криптографическая защита - защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

Криптографические ключи – общее название Ключа ЭП и Ключа проверки ЭП.

Сертификат (Сертификат открытого ключа, Сертификат ключа проверки ЭП) – электронный документ, выданный ЦЦС либо доверенным лицом ЦЦС, и подтверждающий принадлежность Ключа проверки ЭП Владельцу сертификата. Сертификаты ЦЦС являются Квалифицированными сертификатами.

Список отозванных сертификатов (СОС) - перечень серийных номеров Сертификатов, выведенных из обращения (аннулированных); формируется ЦЦС и заверяется ЭП Администратора ЦЦС.

Справочник сертификатов - субъект инфраструктуры PKI, обеспечивающий хранение Сертификатов и Списков отозванных сертификатов (СОС), формируемых в ЦЦС.

Средство криптографической защиты информации (СКЗИ) - средство криптографической защиты информации, включающее библиотеку криптографических преобразований и комплекс вспомогательных программных модулей.

Средства ЭП - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание ЭП, проверка ЭП, создание Ключа ЭП и Ключа проверки ЭП.

Средства ЦЦС - программные и (или) аппаратные средства, используемые для реализации функций ЦЦС.

ЦЦС, Центр Цифровых Сертификатов «BeSafe.ru», ЦЦС «BeSafe.ru» – Удостоверяющий центр (Закрытое акционерное общество «Центр Цифровых Сертификатов», сокращенное наименование ЗАО «ЦЦС», ИНН 5407187087, ОГРН 1025403189602), осуществляющий функции по созданию и выдаче Сертификатов, а также иные функции, предусмотренные Федеральным Законом РФ от 06.04.2011г. №63-ФЗ "Об электронной подписи".

Шифрование информации (шифрование) – взаимно-однозначное математическое (криптографическое) преобразование информации, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации блок зашифрованной информации.

ЭП (Электронная подпись) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Видами Электронных подписей, отношения в области использования которых регулируются Федеральным законом РФ от 06.04.2011г. №63-ФЗ «Об электронной подписи», являются простая и усиленная ЭП.

Public Key Cryptography Standards (PKCS) – стандарты криптографии с Открытым ключом.

PKCS#10 – стандарт, определяющий формат и синтаксис «самоподписанного», т.е. подписанного сертифицируемым Ключом ЭП, Запроса на сертификат.

1.2. Общие сведения о Правилах

1.2.1. Настоящие Правила содержат общий набор правил, описывающих порядок выпуска и обслуживания ЦЦС Сертификатов Владельцев сертификатов, присоединившихся к Правилам в порядке, предусмотренном статьей 428 ГК РФ. Настоящие Правила являются соглашением, налагающим обязательства на все вовлеченные стороны, а также служат средством официального уведомления и информирования всех сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг ЦЦС

1.2.2. Правила разработаны в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, а их структура и содержание соответствуют требованиям рекомендации RFC 3647 («Internet X.509 Public Key Infrastructure.Certificate Policy and Certification Practices Framework»).

1.2.3. Правила и уведомления об их изменениях распространяются в электронном виде путем публикации в сети Интернет по адресу: https://besafe.ru. Изменения в Правила вносятся ЦЦС в одностороннем порядке и вступают в силу по истечении 14 (Четырнадцати) дней с момента размещения их новой редакции по адресу https://besafe.ru.

1.2.4. Тарифы и условия оплаты вознаграждения ЦЦС публикуются в сети Интернет по адресу bank.faktura.ru. ЦЦС имеет право изменять Тарифы и условия оплаты вознаграждения в сроки, аналогичные п. 1.2.3 настоящих Правил, разместив новые тарифы по адресу bank.faktura.ru. В случае, когда изменение Тарифов вызвано изменением стоимости оказания услуг партнеров ЦЦС, допускается сокращение срока размещения Тарифов до 5 (Пяти) календарных дней до даты их вступления в силу.

1.2.5. В случае прекращения действия Правил ЦЦС уведомляет об этом за 30 (тридцать) календарных дней до даты прекращения их действия. Прекращение действия Правил не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Правил, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

1.2.6. Сторонами в споре, в случае его возникновения, считаются ЦЦС и Владелец сертификата, присоединившийся к Правилам. При рассмотрении спорных вопросов, связанных с настоящими Правилами, Стороны будут руководствоваться действующим законодательством Российской Федерации.

1.2.7. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров. Спорные вопросы между Сторонами, не урегулированные в процессе переговоров, решаются в Арбитражном суде Новосибирской области в соответствии с действующим законодательством Российской Федерации.

1.2.8. Деятельность ЦЦС может быть прекращена в порядке, установленном законодательством Российской Федерации. В случае прекращения деятельности ЦЦС, Владельцы сертификатов, срок действия которых еще не истек, должны быть извещены об этом в письменной форме за 1 (один) месяц до даты прекращения деятельности ЦЦС.

1.2.9. В связи с прекращением деятельности ЦЦС Сертификаты аннулируются (отзываются) или передаются лицу, к которому перешли функции ЦЦС, в порядке, определенном ч.6, ст.13 и ч.4, ст.15 №63-ФЗ «Об электронной подписи».

2. Основные положения

2.1. Удостоверяющий центр

2.1.1. В инфраструктуре ЦЦС выполнение всех услуг по управлению Ключами проверки ЭП и Сертификатами Владельцев сертификатов осуществляется с помощью сертифицированного ФСБ России программно-аппаратного комплекса (ПАК) «Удостоверяющий центр «КриптоПро УЦ» версии 1.5.

2.1.2. Сертификаты уполномоченных лиц ЦЦС зарегистрированы в Едином государственном реестре сертификатов ключей подписи удостоверяющих центров, а Квалифицированные сертификаты уполномоченных лиц ЦЦС внесены в реестр сертификатов аккредитованных удостоверяющих центров.

2.1.3. Владельцы сертификатов признают, что криптографические приложения, построенные на базе сертифицированных ФСБ России СКЗИ, используемые для организации PKI и построения

защищенных сервисов, обеспечивают необходимый уровень безопасности при защите информации, не составляющей государственную тайну.

2.1.4. Владельцы сертификатов при работе с защищенными сервисами не могут использовать Ключи ЭП и соответствующие им Сертификаты по истечении периода их действия. Окончание периода действия Сертификатов автоматически контролируется криптографическими приложениями, построенными на базе СКЗИ.

2.1.5. Владельцы сертификатов обязуются соблюдать требования федерального законодательства и локальных нормативных актов в части эксплуатации СКЗИ и наличия лицензий. В процессе эксплуатации СКЗИ Владельцы сертификатов обязуются соблюдать лицензионные ограничения разработчика СКЗИ и программных средств для работы с Сертификатами, а также выполнять рекомендации по обеспечению безопасности информации при эксплуатации СКЗИ.

2.1.6. ЦЦС обеспечивает Владельцам сертификатов возможность получения в форме электронных документов любых Сертификатов, выпущенных ЦЦС, в течение всего срока их действия.

2.1.7. ЦЦС обеспечивает выполнение следующих функций:

- формирование Криптографических ключей ЦЦС (уполномоченных лиц ЦЦС);
- формирование корневых Сертификатов ЦЦС;
- регистрация в реестре ЦЦС Владельцев сертификатов;
- прием и регистрацию Запросов Сертификата;
- контроль уникальности Ключей проверки ЭП в регистрируемых запросах;
- изготовление на основании Запросов электронных Сертификатов;
- аутентификация Владельцев сертификатов, запрашивающих аннулирование (отзыв) Сертификатов;
- аннулирование (отзыв) Сертификатов по запросам, поступающим от Владельцев сертификатов и Регистрационных центров;
- выпуск Списка отозванных сертификатов (СОС);
- ведение реестра выпущенных Сертификатов открытых ключей и СОС;
- публикация реестра выпущенных Сертификатов и СОС в общедоступном сетевом справочнике;
- подтверждение подлинности ЭП в документах, представленных в электронной форме, по запросам Владельцев сертификатов;
- хранение Запросов сертификата и Сертификатов в реестре Сертификатов в течение 5 (Пяти) лет для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с их применением;
- формирование запросов с Ключами проверки ЭП ЦЦС для кросс-сертификации в других Удостоверяющих центрах или для сертификации в вышестоящем Удостоверяющем центре (по договоренности);
- выпуск кросс-сертификатов ключей проверки ЭП для внешних по отношению к ЦЦС Удостоверяющих центров других систем PKI (по договоренности);
- регистрацию, выпуск Сертификатов и назначение полномочий для Агентов.

2.2. Агенты

2.2.1. Агенты выступают в роли уполномоченных представителей ЦЦС. Агент регистрирует запросы на выпуск и отзыв Сертификатов, обеспечивает их доставку в ЦЦС и отвечает за

передачу сформированных Сертификатов Владельцам. Агент работает на основании Соглашения о присоединении к Правилам ЦЦС (Приложение 1 к настоящим Правилам).

2.2.2. В процессе своей деятельности Агент реализует следующие функции:

- первичная идентификация и аутентификация Владельцев сертификатов;
- регистрация Владельцев сертификатов;
- предоставление Владельцам сертификатов программных или программно-аппаратных средств для генерации Ключей ЭП и Запросов сертификата, а также программного обеспечения, необходимого для работы в защищенных прикладных системах.
- формирование Запросов сертификата по заявкам Владельцев сертификатов; во избежание конфликтных ситуаций, которые могут возникнуть при централизованном хранении Ключей ЭП Владельцев сертификатов, Агент не оказывает услуг по их депонированию. Особенности взаимодействия ЦЦС и Агента по вопросам создания Сертификатов для нужд Агента и поставки Смарт-ключей Агенту указаны в Приложении №2 к настоящим Правилам;
- прием Запросов на сертификаты от Владельцев сертификатов;
- предоставление Владельцам сертификатов изготовленных Сертификатов в электронной форме;
- аутентификация Владельцев сертификатов, запрашивающих аннулирование (отзыв) Сертификатов;
- прием запросов на аннулирование (отзыв) Сертификатов от Владельцев сертификатов и передача их в ЦЦС;

2.3. Справочник сертификатов

В инфраструктуре ЦЦС выданные Сертификаты публикуются в специализированный справочник. Информация, публикуемая в справочнике, пополняется из реестра ЦЦС. Внесение изменений в справочник с целью публикации новых Сертификатов и СОС выполняется в ЦЦС автоматически, при их формировании. Доступ к справочнику имеют все Владельцы сертификатов.

2.4. ПРАВА ЦЦС И ВЛАДЕЛЬЦЕВ СЕРТИФИКАТА

2.4.1. Права ЦЦС

ЦЦС, в том числе в лице своих уполномоченных представителей – Агентов - имеет право:

- Требовать у Владельцев сертификатов подтверждения достоверности информации, содержащейся в Сертификатах.
- Вносить в реестр выданных Сертификатов ЦЦС регистрационную информацию о Владельцах сертификатов (в объеме обязательных атрибутов поля идентификационных данных Владельца сертификата).
- Отказать физическому либо юридическому лицу в регистрации в ЦЦС в случае ненадлежащего оформления необходимых регистрационных документов, а также в случае, когда подлинность документов вызывает сомнение.
- Отказать физическому либо юридическому лицу в изготовлении Сертификата в случае ненадлежащего оформления заявления на изготовление Сертификата.
- Отказать физическому либо юридическому лицу в изготовлении Сертификата по иным причинам, не описанным в разделе 2.4.1 настоящих Правил.
- Отказать в аннулировании (отзыве) Сертификата в случае ненадлежащего оформления заявления на аннулирование (отзыв) Сертификата, а также в случае, если истек установленный срок действия этого Сертификата.
- Аннулировать (отозвать) Сертификат в случае:

1. письменного обращения Владельца сертификата;
2. установленного факта компрометации соответствующего ему Ключа ЭП, с уведомлением Владельца аннулированного (отозванного) сертификата и указанием обоснованных причин;
3. если ЦЦС стало известно о прекращении действия документа, на основании которого оформлен Сертификат;
4. указания лиц или органов, имеющих такое право в силу закона.

- По обращению Владельца сертификата выступать в качестве эксперта по вопросам применения СКЗИ в случае возникновения споров между Владельцами сертификатов.
- В случае прекращения действия настоящих Правил аннулировать (отозвать) Сертификаты.

2.4.2. Права Владельцев сертификатов

Владелец сертификата имеет право:

1. Получить Сертификат уполномоченного лица ЦЦС, применять его для проверки ЭП уполномоченного лица ЦЦС в Сертификатах, изготовленных в ЦЦС
2. Получить Список отозванных сертификатов, изготовленный в ЦЦС.
3. Применять Список отозванных сертификатов, изготовленный в ЦЦС, для проверки статуса Сертификатов, изготовленных в ЦЦС.
4. Применять свой Сертификат для проверки ЭП электронных документов в соответствии со сведениями, указанными в Сертификате.
5. Обратиться к ЦЦС или Агенту для аннулирования (отзыва) Сертификата, если период действия этого Сертификата еще не истек.
6. Обратиться к ЦЦС или Агенту за подтверждением подлинности ЭП, связанных с использованием Сертификатов, выданных ЦЦС в документах, представленных в электронной форме.
7. Обратиться к Агенту для приобретения средств ЭП (включая средства генерации Ключей ЭП и Запросов сертификата).
8. Обратиться к Агенту с заявлением на формирование Ключа ЭП и изготовление Сертификата с записью их на ключевой носитель.

2.5. ОБЯЗАННОСТИ ЦЦС, АГЕНТОВ И ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ

2.5.1.Обязанности ЦЦС

ЦЦС обязан:

в отношении Ключей ЭП и Сертификатов ЦЦС

- обеспечивать формирование Ключа ЭП и изготовление Сертификата уполномоченного лица ЦЦС только с помощью СКЗИ;
- использовать Ключ ЭП уполномоченного лица ЦЦС только для заверения издаваемых им Сертификатов и Списков отозванных сертификатов;
- обеспечивать надежную защиту Ключа ЭП уполномоченного лица ЦЦС от несанкционированного доступа;

в отношении регистрации Владельцев сертификатов

- осуществлять регистрацию Владельцев сертификатов в реестре ЦЦС по их заявлениям на регистрацию;

- осуществлять первичную идентификацию и аутентификацию Владельцев сертификатов в соответствии с положениями настоящих Правил;
- хранить следующие данные:

  1) реквизиты основного документа, удостоверяющего личность Владельца сертификата;

  2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право уполномоченного представителя юридического лица обращаться за получением Сертификата;

  3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия Владельца сертификата действовать по поручению третьих лиц, если информация о таких полномочиях Владельца сертификата включена в Сертификат;
- обеспечить Владельцам сертификата безвозмездный доступ с использованием сети Интернет к выданным ЦЦС Сертификатам (затраты на подключение к сети Интернет несет Владелец сертификата);

в отношении изготовления Сертификатов:

- принимать и обрабатывать запросы на сертификацию и выпускать новые Сертификаты:
  - осуществлять регистрацию поступающих Запросов сертификата;
  - осуществлять изготовление Сертификатов на основании и в соответствии с Запросами сертификата;
  - обеспечивать уникальность регистрационной информации Владельца сертификата, включаемой в атрибуты Сертификата;
  - соблюдать конфиденциальность в отношении регистрационной информации о Владельце сертификата:
  - обеспечивать уникальность серийных номеров изготавливаемых Сертификатов:
  - вести реестр выпущенных Сертификатов;
  - уведомлять Владельца сертификата о выпуске запрошенного им Сертификата;
  - обеспечить архивное хранение Сертификатов в электронном виде в течение всего срока действия Сертификатов;
  - обеспечивать архивное хранение Сертификатов в течение 5 лет после их аннулирования (отзыва) или окончания срока действия для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с их применением;
- публиковать реестр выпущенных Сертификатов;

в отношении отзыва Сертификатов

- принимать и обрабатывать запросы от Владельцев сертификатов на отзыв Сертификатов:
  - принимать и обрабатывать запросы на отзыв Сертификатов;
  - отзывать Сертификаты по запросам Владельцев сертификатов или Агента;
- уведомлять Владельца сертификата о фактах, которые стали известны ЦЦС и которые существенным образом могут сказаться на возможности дальнейшего использования его Сертификатов;

в отношении справочника Сертификатов

- обеспечивать своевременную публикацию Сертификатов и СОС;

в отношении синхронизации времени

- обеспечивать работу служб ЦЦС по UTC (Всемирному координированному времени) с учетом часового пояса.

- обеспечивать синхронизацию по времени всех программных и технических средств ЦЦС в соответствии с их предназначением;

в отношении оказания дополнительных услуг

- по запросам Владельцев сертификатов обеспечивать подтверждение подлинности ЭП в документах, представленных в электронной форме;
- консультировать Агентов по вопросам, связанным с использованием Сертификата.

2.5.2.Обязанности АГЕНТА

АГЕНТЫ обязаны:

- осуществлять регистрацию Владельцев сертификатов по их заявлениям на регистрацию;
- осуществлять первичную идентификацию и аутентификацию Владельцев сертификатов в соответствии с положениями настоящих Правил;
- обеспечивать конфиденциальность в отношении изготовляемых Ключей ЭП;
- осуществлять регистрацию поступающих Запросов сертификата и передавать их по защищенному каналу в ЦЦС;
- передавать полученные из ЦЦС сформированные Сертификаты Владельцам;
- принимать запросы на аннулирование (отзыв) скомпрометированных Сертификатов и передавать их по каналу защищенного взаимодействия в ЦЦС;
- аутентифицировать Владельца сертификата, запрашивающего аннулирование (отзыв) Сертификата;
- консультировать Владельцев сертификатов по всем вопросам, связанным с использованием Сертификата (консультирование осуществляется в порядке обмена Сторонами электронными сообщениями).

2.5.3. Обязанности Владельцев сертификатов

Владельцы сертификатов должны строго соблюдать правила, изложенные в настоящих Правилах, в частности:

- обеспечивать сохранность Ключа ЭП и ключевого носителя, принимать все возможные меры для предотвращения их потери, раскрытия, модифицирования или несанкционированного использования;
- в случае обнаружения Компрометации ключей незамедлительно сообщить ЦЦС или Агенту о факте компрометации, прекратить использование Ключей ЭП и прислать в ЦЦС или Агенту запрос на аннулирование (отзыв) Сертификата;
- не использовать Ключи ЭП и соответствующие им Сертификаты по истечении срока их действия, за исключением случаев архивной проверки подписи;
- своевременно осуществлять смену Ключа ЭП;
- точно соблюдать формат и структуру Запроса сертификата, предоставляемого Агенту;
- предоставлять Агенту регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящих Правил;
- указывать в Запросе сертификата максимально точные и действительные сведения;
- подтверждать по требованию ЦЦС или Агента достоверность информации, содержащейся в Сертификате, выдаваемом Владельцу сертификата;
- использовать Сертификат исключительно в соответствии с назначением Сертификата, определенным соответствующими полями расширения в Сертификате;
- своевременно (до истечения периода действия Сертификата) осуществлять смену Ключа ЭП и Сертификата;

- своевременно информировать Агента о фактах изменения персональных данных содержащихся в Сертификатах;
- соблюдать положения настоящих Правил.

2.6. ОТВЕТСТВЕННОСТЬ ЦЦС, АГЕНТОВ И ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ

2.6.1.Ответственность ЦЦС

ЦЦС несет ответственность:

- за обеспечение конфиденциальности Ключей ЭП уполномоченного лица ЦЦС;
- за соблюдение порядка и сроков формирования Сертификатов и СОС,
- за соблюдение сроков отзыва выпущенных Сертификатов.

ЦЦС не несет ответственности за любые прямые или косвенные убытки, любую потерю прибыли, явившиеся результатом:

- несоблюдения Владельцами сертификатов конфиденциальности собственных Ключей ЭП, а также достоверности и целостности Сертификатов Администраторов ЦЦС;
- несвоевременного уведомления о Компрометации ключа Владельца сертификата;
- нарушения Владельцами сертификатов положений настоящих Правил.

2.6.2.Ответственность Агентов

АГЕНТЫ в качестве уполномоченных представителей ЦЦС отвечают:

- за соответствие данных в Запросе сертификата и в подтверждающих документах, представленных физическими / юридическими лицами на регистрацию в ЦЦС;
- за обеспечение конфиденциальности Ключей ЭП Владельцев выпускаемых сертификатов (в случае формирования Ключей ЭП Владельцев сертификатов средствами Агента).

2.6.3.Ответственность Владельцев сертификатов

Сведения об ответственности Владельцев сертификатов за выполнение возложенных на них обязательств изложены в соглашениях (договорах) с участниками обслуживаемых PKI систем.

2.7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Конфиденциальной считается любая информация о Владельце сертификата, не включенная в состав Сертификатов, формируемых ЦЦС:

- Ключ ЭП, соответствующий Ключу проверки ЭП Владельца сертификата;
- реестры ЦЦС, за исключением Справочника сертификатов;
- отчет о проведении процедуры проверки подлинности ЭП в электронном документе;
- персональные данные Владельцев сертификатов, не подлежащие включению в Сертификат;
- информация, конфиденциальность которой охраняется ЦЦС в соответствии с договорами и локальными нормативными актами ЦЦС.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией:

- информация о настоящих Правилах;
- сведения, включаемые в Сертификаты и Списки отозванных сертификатов, издаваемые ЦЦС;
- актуальный Список отозванных (аннулированных) Сертификатов и актуальный справочник Сертификатов.

Открытая информация может публиковаться по решению администрации ЦЦС. Место, способ и время публикации открытой информации определяется ЦЦС.

Передача конфиденциальной информации третьим лицам и уполномоченным органам государственной власти осуществляется в соответствии с действующим законодательством Российской Федерации.

2.8. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

2.8.1.Система именования. Уникальность имен

Имена Сертификатов, используемые для идентификации и аутентификации Владельцев сертификатов, должны соответствовать требованиям, изложенным в Федеральном законе №63-ФЗ «Об электронной подписи» и в RFC 5280.

Уникальность имен, присваиваемых участникам обслуживаемых систем и используемых в составе формируемых Сертификатов, обеспечивается средствами ЦЦС.

2.8.2.Первичная идентификация и аутентификация Владельцев сертификата.

Идентификация физического/юридического лица выполняется в процессе его регистрации в ЦЦС «BeSafe» или у Агента. Результатом идентификации является присвоение Владельцу сертификата уникального имени и занесение данного имени в реестр зарегистрированных Владельцев сертификата.

Уникальные имена Владельцев сертификата формируются на основании идентификационных данных, указанных в заявлении на изготовление Сертификата.

Имя Владельца сертификата - юридического лица должно включать полное наименование данной организации и имя уполномоченного представителя (сотрудника) организации. Для этого уполномоченный представитель при регистрации в ЦЦС должен предоставить Агенту письменный документ, оформленный и заверенный надлежащим образом, подтверждающий право представителя получить и использовать сертификат в соответствии с его назначением (например, доверенность).

Начальная аутентификация физического лица производится с использованием документа, удостоверяющего личность.

2.8.3.Идентификация и аутентификация зарегистрированного Владельца сертификата

Идентификация зарегистрированного Владельца сертификата осуществляется по уникальному имени (идентификатору Владельца сертификата), занесенному в реестр ЦЦС при первичной регистрации Владельца сертификата.

Аутентификация зарегистрированного Владельца сертификата выполняется по паспорту или другому документу, удостоверяющему личность, предъявляемому лично.

Удаленная аутентификация зарегистрированного Владельца сертификата по Сертификату осуществляется путем выполнения процедуры проверки ЭП в электронном документе с использованием Сертификата.

3. Порядок действия Владельца сертификата при первичной генерации Ключей ЭП и изготовлении клиентских и серверных Сертификатов

3.1. ЦЦС осуществляет изготовление Сертификатов для физических и юридических лиц (в лице уполномоченных представителей) без привлечения Агента только по соглашению сторон, и только в том случае, если указанное лицо (Владелец сертификата) присоединилось к Правилам ЦЦС, заключило Договор на изготовление и обслуживание Сертификатов с ЦЦС и оплатило услуги, связанные с изготовлением Сертификата.

3.2. Сформировать Заявку на оказание услуг ЦЦС (первичную генерацию Ключей ЭП, выдачу Сертификатов) можно одним из следующих способов:

- удаленно посредством использования специализированного программного обеспечения;

- лично при обращении заинтересованного лица к Агенту (способ доступен при наличии технической возможности).

3.3. Если формирование Ключей ЭП и Запросов сертификата Владелец сертификата будет выполнять самостоятельно, Заявка должна быть оформлена с использованием программного обеспечения ЦЦС, ссылка на доступ к которому предоставляется Владельцу сертификата Агентом.

3.4. В ЦЦС допускается два способа генерации Ключей ЭП и Запросов на сертификаты:

1. **самостоятельно Владельцем сертификата** на своем рабочем месте; генерация Ключей ЭП и Запросов сертификата выполняется в этом случае с помощью программного обеспечения, доступ к которому предоставляется Владельцу сертификата Агентом;
2. **доверенным лицом Агента,** на специально оборудованном АРМ, соответствующем требованиям ФСТЭК России по технической защите конфиденциальной информации (при наличии технической возможности).

3.5. Изготовление Сертификата при самостоятельном выполнении процедуры генерации Ключей ЭП и Запросов сертификата Владельцем сертификата:

- Владелец сертификата с помощью ПО для генерации Ключей ЭП и Запроса сертификата формирует Ключ ЭП на ключевой носитель, предоставленный Агентом (смарт-ключ с неизвлекаемым Ключом ЭП), и Запрос на сертификат («самоподписанный» запрос формата PKCS#10);
- средствами ПО для генерации Ключей ЭП и Запросов сертификата Владелец сертификата направляет в электронном виде Запрос сертификата Агенту;
- средствами ПО для генерации Ключей ЭП и Запросов сертификата Владелец сертификата распечатывает Заявление на выдачу Квалифицированного сертификата ключа проверки электронной подписи и заверяет его собственноручной подписью и печатью (при наличии);
- Заявление на выдачу Квалифицированного сертификата в бумажном виде Владелец сертификата передает Агенту;

3.6. Для формирования Ключей ЭП и изготовления Сертификатов Владельцу сертификата необходимо подготовить и представить Агенту комплект документов:

- Заявление на выдачу Квалифицированного сертификата по форме Приложений 5, 7 к настоящим Правилам, подписанное собственноручно Владельцем сертификата, а для юридических лиц – уполномоченным лицом Владельца сертификата;
- основной документ, удостоверяющий личность, страховое свидетельство государственного пенсионного страхования заявителя - физического лица или учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя - юридического лица;
- надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);
- доверенность или иной документ, подтверждающий право уполномоченного представителя действовать от имени других лиц и заверяющий должностные полномочия уполномоченных представителей в рамках своей организации;

3.7. Ответственность за полноту и достоверность информации, указанной в •Заявлении на выдачу Квалифицированного сертификата, несет заявитель.

3.8. Комплект указанных в п.3.6 настоящих Правил документов передается Агенту при личном визите Владельца сертификата к Агенту.

3.9. Изготовление Сертификата при личном обращении

3.9.1. Сотрудник Агента идентифицирует личность заявителя по паспорту или иному документу, удостоверяющему личность.

3.9.2. Сотрудник Агента принимает документы, проверяет соответствие персональных данных, указанных в Заявлении на выдачу Квалифицированного сертификата, представленным паспортным данным или заверенным сведениям.

3.9.3. Если генерация Ключей ЭП и формирование Запросов сертификата выполнялись Владельцем сертификата самостоятельно, сотрудник Агента проверяет соответствие персональных данных и прочих реквизитов, указанных в Заявлении на выдачу Квалифицированного сертификата, представленным данным.

3.9.4. В случае отказа в регистрации и изготовлении Сертификата Заявление на выдачу Квалифицированного сертификата, возвращается Владельцу сертификата, с указанием причины отказа.

3.9.5. В случае принятия положительного решения сотрудник Агента в течение 4 (Четырех) часов с момента приема документов, указанных в п.3.8, выполняет процедуру занесения регистрационной информации в реестр ЦЦС.

3.9.6. Сотрудник Агента выполняет формирование Ключей ЭП и Запросов сертификата в соответствии со следующими положениями настоящих Правил:

- сформированный Ключ записываются на отчуждаемый ключевой носитель, приобретенный у Агента;
- ключевой носитель, содержащий изготовленный Ключ ЭП, передается Владельцу сертификата лично; факт выдачи Ключа ЭП заносится в Журнал учета изготовления и выдачи Ключей ЭП и заверяется собственноручной подписью Владельца сертификата;
- Запрос Сертификата экспортируется в ЦЦС средствами предоставленного ЦЦС Агенту программного обеспечения

3.9.7. На основании поступившего Запроса на сертификат, ЦЦС изготавливает Сертификат в электронной форме, автоматически помещает его в сетевой Справочник сертификатов ЦЦС и уведомляет Владельца сертификата об изготовлении Сертификата по адресу электронной почты, включенному в состав соответствующего Запроса сертификата.

3.9.8. Сотрудник Агента распечатывает на бумажном носителе две копии Акта приема-передачи Сертификата (по форме Приложений 6,8 к настоящим Правилам), проставляет собственноручную подпись уполномоченного лица Агента и печать Агента (при наличии).

3.9.9. Владелец сертификата проставляет собственноручную подпись и печать (при наличии) на Актах приема-передачи Сертификата.

3.9.10. По окончании процедуры изготовления Сертификата Владельцу сертификата выдаются:

- Ключ ЭП, записанный на отчуждаемый ключевой носитель;
- Сертификат Владельца сертификата в электронной форме, соответствующий его Ключу ЭП;
- Акт приема-передачи Сертификата, заверенный с двух сторон - собственноручной подписью Владельца сертификата и Уполномоченного сотрудника Агента.

Электронная форма Сертификата Владельца сертификата передается Владельцу сертификата в виде файла, записанного на отчуждаемый ключевой носитель.

4. Порядок действий Владельца сертификата при проведении плановой смены Ключей ЭП и обновлении клиентских и серверных Сертификатов

4.1. Не позднее, чем за 2 (Две) недели до окончания периода действия текущего рабочего Ключа ЭП Владельца сертификата, он должен обратиться к Агенту за формированием нового Ключа ЭП и Сертификата.

4.2. Дальнейший Порядок действий Владельца сертификата при проведении плановой смены Ключей ЭП и Сертификатов соответствует порядку действий при первичном изготовлении Сертификата на основании электронной формы «самоподписанного» запроса формата PKCS#10.

4.3. При самостоятельном изготовлении новых Ключей ЭП и оформлении Запроса на обновление сертификата (по Заявлению на выдачу Квалифицированного сертификата) Владелец сертификата

может сформировать запрос формата PKCS#10 с новым Ключом проверки ЭП, подписанный его текущим Ключом ЭП.

4.5. Если к моменту плановой смены ключей атрибуты Владельца сертификата, включаемые в состав нового Сертификата, не изменились и совпадают с атрибутами действующего Сертификата, запрос на обновление Сертификата передается в ЦЦС без необходимости передачи подтверждающих документов в бумажном виде, при этом Сертификат формируется и публикуется в Справочнике сертификатов ЦЦС автоматически, в режиме on-line.

4.6. При изменении атрибутов в запросе на новый Сертификат изготовление Сертификата производится в соответствии с разделом 3 настоящих Правил, как при первичной регистрации.

4.8. Об изготовлении нового Сертификата Владелец сертификата уведомляется по адресу электронной почты, включенному в состав Сертификата.

4.7. По ссылке, полученной вместе с уведомлением об изготовлении Сертификата, Владелец сертификата скачивает свой Сертификат. Хранение Сертификата необходимо осуществлять на отчуждаемом ключевом носителе (с неизвлекаемыми закрытыми ключами). С момента получения Сертификата ключевой носитель с соответствующим Ключом ЭП становится рабочим ключевым носителем.

4.8. Ключевые носители с Ключами ЭП, срок действия которых истек, должны уничтожаться путем двойного переформатирования.

5. Отзыв Сертификата Владельца сертификата

5.1. В ЦЦС Сертификат Владельца сертификата изымается из обращения (отзывается) в следующих случаях:

- по истечении периода действия Сертификата;
- при Компрометации ключа (см. п.6.1);
- в случае изменения атрибутов в Сертификате, по заявлению Владельца сертификата в письменной форме, а для юридических лиц – заявлению, заверенному руководителем организации Владельца сертификата;
- в случае обнаружения ЦЦС факта изменения атрибутов в Сертификате Владельца сертификата;
- в случае заявления Владельца сертификата о прекращении Договора на обслуживание в ЦЦС.

5.2. Отзыв Сертификатов Владельцев сертификатов может также осуществляться по инициативе ЦЦС в случаях истечения одного из следующих сроков:

- срока полномочий Владельца сертификата;
- срока действия иного документа, на основании которого был оформлен Сертификат Владельца сертификата.

5.3. В случае отзыва Сертификата Владельца сертификата Администратор ЦЦС помещает его серийный номер в Список Отозванных Сертификатов (СОС) с указанием причины отзыва и публикует СОС в справочнике Сертификатов ЦЦС.

5.4. Обработка заявления на отзыв Сертификата Владельца сертификата, выпуск и публикация СОС в справочнике Сертификатов ЦЦС, а также уведомление Владельца об аннулировании (отзыве) Сертификата должны быть осуществлены не позднее 12 часов с момента регистрации заявления в ЦЦС.

5.5. Дата, с которой Сертификат считается недействительным, устанавливается равной дате формирования СОС, в который был включен серийный номер отозванного Сертификата.

5.6. Сертификаты с истекшим периодом действия не заносятся в СОС, т.к. криптографические приложения автоматически прекращают действия с просроченными Сертификатами.

6. Порядок действий Владельца сертификата при Компрометации ключа

6.1. К событиям, на основании которых Владелец сертификата приходит к выводу о компрометации своего Ключа ЭП, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- для юридических лиц: увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение при работе в защищенном сервисе;
- нарушение правил хранения ключевых носителей.

6.2. В случае принятия решения о Компрометации ключа Владелец сертификата обязан прекратить его использование, заполнить заявку на отзыв Сертификата и направить ее в ЦЦС или Агенту.

6.3. Получив от Владельца сертификата сообщение о Компрометации ключа, Администратор ЦЦС помещает серийный номер соответствующего Сертификата в СОС с причиной отзыва "Компрометация ключей" и немедленно публикует его в справочнике сертификатов ЦЦС.

7. Дополнительные положения

7.1. Требования к Средствам ЭП Владельцев сертификатов

Средство ЭП должно обеспечивать выполнение следующих процедур:

- генерацию Криптографических ключей;
- формирование ЭП;
- проверку ЭП.

В качестве Средства ЭП Владельцы сертификатов должны использовать ПО, разработанное с использованием сертифицированных в соответствии с правилами сертификации средств криптографической защиты информации по уровню защиты КС1, КС2.

7.2. Сроки действия Ключей ЭП и Сертификатов

Срок действия Ключа ЭП Владельца сертификата, соответствующего Сертификату, владельцем которого он является, составляет 1 год.

Начало периода действия Ключа ЭП Владельца сертификата исчисляется с даты и времени начала действия соответствующего Сертификата.

Срок действия Ключа проверки ЭП устанавливается равным сроку действия Сертификата.

Срок действия Сертификата устанавливается Удостоверяющим центром в момент его изготовления.

Меры защиты Ключей ЭП

Ключи ЭП Владельцев сертификатов при их генерации должны записываться на отчуждаемые носители ключевой информации с неизвлекаемым ключом (смарт-ключи), предоставляемые ЦЦС через Агентов.

Ключи ЭП на отчуждаемом носителе защищаются паролем. Пароль формирует лицо, выполняющее процедуру генерации Ключей.

Если процедуру генерации ключей Владельца сертификата выполняет сотрудник Агента, то он должен сообщить сформированный пароль Владельцу сертификата.

Ответственность за незамедлительную смену пароля после получения ключевого носителя несет Владелец сертификата.

Требования данного раздела распространяются и на создаваемые резервные копии Ключей ЭП.

Сотрудники Удостоверяющего центра, являющиеся Владельцами сертификатов, также должны выполнять требования данного раздела настоящих Правил.

7.3. Архивное хранение документированной информации

7.3.1. Состав архивных документов

Архивированию подлежит следующая документированная информация:

- реестр Сертификатов Владельцев сертификатов;
- Сертификаты ЦЦС;
- журналы аудита программно-аппаратных средств обеспечения деятельности ЦЦС (если таковые существуют);
- реестр зарегистрированных Владельцев сертификатов;
- заявления на выдачу Квалифицированного сертификата
- акты приема-передачи Сертификата;
- заявления на аннулирование (отзыв) Сертификатов;
- служебные документы ЦЦС.

7.3.2. Срок хранения документации в архивах составляет 5 лет.

8. Структуры Сертификатов и Списка отозванных сертификатов

8.1. Структура Сертификатов, формируемых ЦЦС

ЦЦС формирует Сертификаты Владельцев сертификата в электронной форме формата X.509 версии 3.

8.1.1. Базовые поля Сертификата

Сертификаты содержат следующие базовые поля X.509:

Поле	Описание
Version	версия Сертификата формата X.509
SerialNumber	уникальный серийный (регистрационный) номер Сертификата в реестре Сертификатов ЦЦС
Signature	идентификатор алгоритма подписи
Issuer	идентифицирующие данные ЦЦС
Validity	даты начала и окончания срока действия Сертификата
Subject	идентифицирующие данные Владельца сертификата
SubjectPublicKeyInformation	идентификатор алгоритма и значение Ключа проверки ЭП
extensions	расширения Сертификата

8.1.2. Расширения Сертификата

Сертификаты могут содержать следующие расширения:

Расширение	Описание
AuthorityKeyIdentifier	идентификатор ключа издателя Сертификата
SubjectKeyIdentifier	идентификатор ключа Владельца сертификата
KeyUsage	назначение Криптографического ключа
CertificatePolicies	сертификационные политики
SubjectAlternativeName	альтернативное имя Владельца
IssuerAlternativeName	альтернативное имя издателя
BasicConstraints	основные ограничения
ExtendedKeyUsage	расширенное назначение Криптографического ключа
CRL DistributionPoints	адрес Списка отозванных сертификатов

8.1.2. Объектные идентификаторы алгоритмов

ЦЦС использует следующие идентификаторы алгоритмов Средств ЭП:

Алгоритм	Крипто-КОМ 3.2	RFC 4357
ГОСТ Р 34.10-2001	1.2.6.1.4.1.5849.1.6.2	1.2.643.2.2.19
ГОСТ Р 34.11-94 (для отдельных СКЗИ)	1.2.6.1.4.1.5849.1.2.1	1.2.643.2.2.9

8.1.4. Формы имени

В Сертификате поля идентификационных данных ЦЦС и Владельца сертификата содержат атрибуты имени формата X.500.

8.1.5. Атрибуты имени

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, являются:

Атрибут	Описание
CountryName (C)	страна (код России в Стандарте ISO 3166 - RU)
CommonName (CN)	полное имя (фамилия, имя, отчество)
E-mail	адрес электронной почты

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося юридическим лицом (в лице уполномоченного представителя), являются:

Атрибут	Описание
CountryName(C)	страна (код России в Стандарте ISO 3166 - RU)
StateOrProvinceName (SP)	субъект Российской Федерации, где зарегистрирована организация - Владелец сертификата
LocalityName (L)	город, где зарегистрирована организация - Владелец сертификата
OrganizationName (O)	наименование организации - Владельца сертификата
OrganizationalUnitName (OU)	наименование подразделения организации - Владельца сертификата
CommonName (CN)	полное имя уполномоченного представителя Владельца сертификата (фамилия, имя, отчество)
E-mail	адрес электронной почты уполномоченного представителя Владельца сертификата

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего центра являются:

Атрибут	Описание
CountryName (C)	страна (код России в Стандарте ISO 3166 - RU)
StateOrProvinceName (SP)	субъект Российской Федерации, где зарегистрирована организация - организатор ЦЦС
LocalityName (L)	город, где зарегистрирована организация - организатор ЦЦС
OrganizationName (O)	наименование организации - организатора ЦЦС
CommonName (CN)	наименование ЦЦС
E-mail	адрес электронной почты уполномоченного лица ЦЦС

Ответственность за своевременную актуализацию идентификационных данных Сертификата несет Владелец сертификата.

8.2. Структура Списка отозванных сертификатов, формируемого ЦЦС

ЦЦС издает Списки аннулированных (отозванных) Сертификатов в электронной форме формата X.509 версии 2.

8.2.1. Базовые поля Списка отозванных сертификатов

Списки аннулированных (отозванных) Сертификатов содержат следующие расширения:

Название	Описание
Version	версия COC формата X.509

SignatureAlgorithm	идентификатор алгоритма подписи
Issuer	издатель СОС
thisUpdate	время издания СОС
nextUpdate	время, по которое действителен СОС
revokedCertificates	список аннулированных (отозванных) Сертификатов
crlExtensions	расширения СОС

8.2.2. Расширения Списка отозванных сертификатов

Список аннулированных (отозванных) Сертификатов может содержать следующие расширения:

Расширение	Описание
AuthorityKeyIdentifier	идентификатор Криптографического ключа издателя Списка аннулированных (отозванных) Сертификатов

8.2.3. Расширения записей Списка аннулированных (отозванных) Сертификатов

Записи Списка аннулированных (отозванных) Сертификатов могут содержать следующие расширения:

Расширение	Описание
CRL Reason	причина отзыва Сертификата

В качестве причины отзыва Сертификата могут использоваться следующие значения:

Код	Идентификатор	Причина отзыва	Описание
0	Unspecified	Не указана	Отзыв Сертификата без указания причины отзыва. Не рекомендуется для использования.
1	KeyCompromise	Компрометация ключа	Компрометация ключа Владельца сертификата (утеря, раскрытие, искажение ключа, утеря ключа с последующим обнаружением, факт или подозрение того, что ключ стал известен другим лицам, нарушение правил хранения Ключа ЭП).
2	CACompromise	Компрометация ключа ЦЦС	Компрометация ключа ЦЦС. При отзыве Сертификата ЦЦС могут быть отозваны все Сертификаты, выпущенные с его помощью.
3	AffiliationChanged	Смена владельца	Изменение сведений, указанных в Сертификате (увольнение с работы, перевод на другую должность, смена персональных данных Владельца сертификата, выявление ошибок в реквизитах).
4	Superseded	Смена ключа ЭП	Физическая порча ключевого носителя, невозможность воспроизведения пароля к Ключу ЭП.
5	CessationOfOperation	Прекращение работы ЦЦС	Прекращение деятельности ЦЦС. Устанавливает запрет для Сертификата ЦЦС на выпуск новых Сертификатов Владельцев сертификатов, разрешая только выпуск Списков отозванных сертификатов.
9	PrivilegeWithdrawn	Ограничение привилегий	Изменение должностных обязанностей Владельца сертификата или обстоятельств, на основании которых было предоставлено право подписи.

СОГЛАШЕНИЕ № _____
О ПРИСОЕДИНЕНИИ К ПРАВИЛАМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ЦЦС «BESAFE.RU»

г. Новосибирск «___» _____20__ года

Закрытое акционерное общество «Центр Цифровых Сертификатов», именуемое в дальнейшем «Удостоверяющий центр», в лице Директора _____, действующего на основании Устава, с одной стороны, и_____, именуемое в дальнейшем «Агент», в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о следующем:

1. Предметом Соглашения является присоединение Агента в порядке ст.428 Гражданского кодекса РФ к Правилам работы Удостоверяющего центра ЦЦС «BeSafe.ru», которые расположены в Интернете по адрес https://besafe,ru (далее – «Правила УЦ») и являются неотъемлемой частью настоящего Соглашения.
2. Также Агент присоединяется к Правилам корпоративной информационной Системы «BeSafe», которые расположены в Интернете по адресу https://besafe,ru (далее – «Правила «BeSafe») и являются неотъемлемой частью настоящего Соглашения.
3. Правила «BeSafe» распространяются на Агента в рамках его участия в работе Системы в качестве Агента Удостоверяющего центра на условиях Правил УЦ.
4. Удостоверяющий центр и Агент признают, что:
    a. получение документа, подписанного Электронной подписью (далее – «ЭП») Агента, юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц и оттиском печати Агента. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, ЭП и Сертификат ключа проверки ЭП Агента созданы в соответствии с Правилами «BeSafe»;
    b. получение документа, подписанного Электронной подписью Удостоверяющего центра, юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц Удостоверяющего центра и его оттиском печати. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, ЭП и Сертификат ключа проверки ЭП Удостоверяющего центра созданы в соответствии с Правилами «BeSafe».
5. Настоящее Соглашение вступает в силу от даты его подписания Сторонами.
6. Каждая из Сторон имеет право расторгнуть настоящее Соглашение в одностороннем порядке, предварительно направив уведомление другой Стороне не менее чем за три месяца до его расторжения.

РЕКВИЗИТЫ СТОРОН

УДОСТОВЕРЯЮЩИЙ ЦЕНТР:	**АГЕНТ**
Закрытое акционерное общество «Центр Цифровых Сертификатов» (ЗАО «ЦЦС») Место нахождения: 630055, г. Новосибирск, ул. Мусы Джалиля, д. 11 Почтовый адрес: 630055, г. Новосибирск, ул. Шатурская, 2 Банковские реквизиты: Р/с 40702810300000000075 в РНКО «Платежный Центр» (ООО) БИК 045004832 К/с 30103810100000000832 в Сибирском ГУ Банка России ИНН 5407187087 КПП 540801001	
От Удостоверяющего центра	От Агента
_____ (_____)	_____ (_____)
М.п.	М.п.

Особенности создания Сертификатов для нужд Агентов

1. *ЦЦС* в течение 3 (Трех) рабочих дней с момента подачи представителем *Агента* Заявления по форме Приложения №6 к Правилам, изготавливает и выдает *Сертификат Агенту* для обеспечения работы в качестве *Агента ЦЦС*.
2. После получения *Сертификата Агент* обязан направить в *ЦЦС* Заявление согласно Приложению №3 к настоящим Правилам (Заявление на регистрацию/отзыв прав доступа для *Сертификатов*).
3. Указанные в настоящей статье документы подаются *Агентом* в письменной форме на бумажном носителе с приложением комплекта документов, подтверждающих указанные в Заявлениях сведения.
4. При передаче *ЦЦС Агенту Сертификата*, *ЦЦС* и *Агент* подписывают Акт приема-передачи по форме, указанной в Приложении №8 к Правилам.

Порядок поставки ЦЦС Смарт-ключей Агенту

1. *ЦЦС* предоставляет *Агенту Смарт-ключи* в качестве средства хранения *Ключей ЭП*, Сертификатов.
2. Количество *Смарт-ключей*, подлежащих поставке *ЦЦС Агенту*, определяется в заявлении, направляемом *Агентом в ЦЦС* На основании полученного заявления *Агента, ЦЦС* выставляет *Агенту* счет на оплату. Заявление на поставку *Смарт-ключей*, а также их предперсонализацию, направляются *Агентом* в *ЦЦС* в электронном (сканированном) виде по адресу market@faktura.ru. Форма заявления приведена в Приложении №9 к Правилам.
3. Срок отправки *Смарт-ключей Агенту* составляет не более 2 (Двух) месяцев от даты оплаты *Агентом* счета.
4. Право собственности и риск случайной гибели *Смарт-ключей* переходят к *Агенту* с момента получения им *Смарт-ключей* от транспортной организации (службы экспресс-доставки).
5. Обязательство *ЦЦС* по отправке *Смарт-ключей Агенту* считается выполненным с момента передачи их *Агенту* транспортной организацией (службой экспресс-доставки).
6. Претензии, связанные с качеством *Смарт-ключей, Агент* вправе предъявлять к *ЦЦС*.
7. Создание *Сертификата*, передача его *Агенту* для последующей записи на *Смарт-ключ* осуществляется *ЦЦС* в порядке, установленном настоящими Правилами.
8. Спецификация на *Смарт-ключи*, подлежащие к поставке, размещена в сети Интернет по адресу bank.faktura.ru.

Приложение № 3 к Правилам работы Удостоверяющего центра ЦЦС «BeSafe.ru»
Заявление для ЦЦС от Агента на регистрацию прав сотрудников

Директору ЗАО «ЦЦС»
от <Наименование банка>

ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ/ОТЗЫВ ПРАВ ДОСТУПА ДЛЯ СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКОВ АГЕНТА

Просим провести регистрацию/отзыв прав доступа для Сертификатов ключей проверки электронной подписи (Сертификатов) сотрудников Агента:

№	ФИО	Имя издателя Сертификата	Имя Сертификата	Права доступа	Предоставить/ отозвать	Эл.адрес
1						
2						
3						
4						
5						

Список прав доступа:

Очная выдача/обновление Сертификатов – право позволяет сотруднику Агента проводить выдачу, обновление Сертификатов в интерфейсе АРМ Администратора с правом подписывать акты приема-передачи Сертификатов Клиентам непосредственно в офисе Банка с личным присутствием Клиента или официального представителя Клиента, которому выдается или обновляется Сертификат.

Дистанционная выдача/обновление Сертификатов – право позволяет сотруднику Агента подтверждать запросы, на выдачу или обновление Сертификатов, осуществленные Клиентом посредством Интернет с использованием электронных средств (ПК, КПК и т.п.), в интерфейсе АРМ Администратора с правом подписывать акты приема-передачи Сертификатов клиентам.

Просмотр информации – право позволяет сотруднику Агента просматривать информацию о Сертификатах в интерфейсе АРМ Администратора.

____ _____20___года

_____(должность, реквизиты доверенности)

_____ /_____/
(Ф.И.О.)

М.П.

Директору ЗАО «ЦЦС»
От _____

ЗАЯВЛЕНИЕ НА СБОЙНЫЕ СЕРТИФИКАТЫ

По запросам, посланным нами ___ _____ 20__ г. в Удостоверяющий центр на создание Сертификатов ключей проверки электронной подписи, в связи со сбоями в процессе получения, а именно _____ (указать причину сбоя) _____, нам не удалось получить в пригодном для дальнейшего использования виде следующие сбойные Сертификаты по соответствующим им запросам:

№	Subject / Идентификатор владельца сертификата	Issuer / Поставщик
1	CN= , OU= , O= , L= , C=RU	
2	CN=, OU= , O=, L=, C=RU	

В соответствии с Правилами Удостоверяющего центра, просим исключить из оплаты создание вышеуказанных Сертификатов.

_____ _____20___года

_____(должность, реквизиты доверенности)

_____ /_____ /
(Ф.И.О.)

М.П.

Приложение № 5 к Правилам работы Удостоверяющего центра ЦЦС «BeSafe.ru»
Заявление на выдачу Сертификата (физическое лицо)

Агенту Удостоверяющего центра ЦЦС «BeSafe.ru»

<Наименование *Агента*>

/ в Удостоверяющий центр ЦЦС «BeSafe.ru»

ЗАЯВЛЕНИЕ НА ВЫДАЧУ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Прошу Удостоверяющий центр ЦЦС «BeSafe.ru» изготовить и выдать мне *Квалифицированный сертификат ключа проверки электронной подписи* для физического лица с *Идентификатором владельца сертификата*:_____ (ФИО *Клиента*). Уникальный номер запроса (только для удаленной выдачи):_____.

С Правилами *Электронного документооборота* корпоративной информационной *Системы «BeSafe»* (далее – «*Система «BeSafe»*), которые расположены в сети Интернет по адресу www.besafe.ru ознакомлен(-а), соглас(-ен)(-на) и обязуюсь выполнять.

Признаю, что получение документа, подписанного *Электронной подписью Участника Системы «BeSafe»* (далее – «*Участник*») юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц *Участника* и оттиском печати *Участника*. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ электронной подписи*, *Электронная подпись* и *Квалифицированный сертификат Участника* созданы в соответствии с Правилами *Системы «BeSafe».*

Реквизиты *Клиента*:

ФИО	
Контактный телефон	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных ЗАО «Центр Цифровых сертификатов» и признаю, что персональные данные, заносимые в Сертификаты, относятся к общедоступным персональным данным.

_____(подпись Клиента)/_____ (Ф.И.О. Клиента)

принято *Агентом Удостоверяющего центра / Удостоверяющим центром*:
_____(полное наименование)
_____(дата)
_____(подпись уполномоченного лица)
_____(ФИО уполномоченного лица)
М.П.

Приложение № 6 к Правилам работы Удостоверяющего центра ЦЦС «BeSafe.ru»
Заявление на выдачу Сертификата (юридическое лицо)

Агенту Удостоверяющего центра ЦЦС «BeSafe.ru»

<Наименование *Агента*>

/ в Удостоверяющий центр ЦЦС «BeSafe.ru»

ЗАЯВЛЕНИЕ НА ВЫДАЧУ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Прошу Удостоверяющий центр ЦЦС «BeSafe.ru» создать и выдать уполномоченному лицу организации _____(наименование организации), действующ(-ему)(-ей) на основании _____, *Квалифицированный сертификат ключа проверки электронной подписи* (с *Идентификатором владельца сертификата*:_____ (ФИО уполномоченного лица организации / наименование организации). Уникальный номер запроса (только для удаленной выдачи):_____.

С Правилами *Электронного документооборота* корпоративной информационной *Системы «BeSafe»* (далее – «*Система «BeSafe»*), которые расположены в сети Интернет по адресу www.besafe.ru ознакомлены, согласны и обязуемся выполнять.

Признаем, что получение документа, подписанного *Электронной подписью Участника Системы «BeSafe»* (далее – «*Участник*») юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц *Участника* и оттиском печати *Участника*. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ электронной подписи*, *Электронная подпись* и *Сертификат ключа проверки электронной подписи Участника* созданы в соответствии с Правилами *Системы «BeSafe»*.

Реквизиты *Клиента*:

ФИО уполномоченного лица организации	
Наименование организации	
Контактный телефон	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных ЗАО «Центр Цифровых сертификатов» и признаю, что персональные данные, заносимые в Сертификаты, относятся к общедоступным персональным данным.

_____(подпись уполномоченного лица организации)

_____ (Ф.И.О. уполномоченного лица организации)

М.П. (если применимо)

принято *Агентом Удостоверяющего центра / Удостоверяющим центром*:
_____(полное наименование)
_____(дата)
_____(подпись уполномоченного лица)
_____(ФИО уполномоченного лица)
М.П.

М.П.

АКТ ПРИЕМА - ПЕРЕДАЧИ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

<Город> <Дата создания акта>

<ФИО, введенные при выдаче *Сертификата*>, именуем(-ый)(-ая) в дальнейшем «*Владелец сертификата*», с одной стороны, и <Наименование *Агента*> , именуемое в дальнейшем «*Агент*», в лице <должность и ФИО уполномоченного сотрудника Банка >, действующ(-его)(-ей) на основании <документ >, с другой стороны, в соответствии с Правилами работы *Удостоверяющего центра* ЦЦС «BeSafe.ru» составили настоящий Акт приема - передачи о следующем:

1. *Агент* произвел проверку данных *Владельца сертификата*, *Удостоверяющий центр* осуществил изготовление *Сертификата ключа проверки электронной подписи (далее – «Сертификат»)* и передал ДД.ММ.ГГГГ *Сертификат Владельцу сертификата*, а *Владелец сертификата* принял оригинал следующего *Сертификата* на *Ключевой носитель*:

Идентификатор владельца сертификата	CN= , OU= , O= , L= , C=
Номер *Сертификата*	
Алгоритм подписи	
Заверен	
Годен с	
Годен до	
Алгоритм *Ключа проверки электронной подписи*	
Ключ проверки электронной подписи	
Алгоритм отпечатка	
Отпечаток	

2. Обязательства *Агента* перед *Владельцем сертификата* выполнены в точном соответствии с Правилами работы *Удостоверяющего центра* ЦЦС «BeSafe.ru», претензий у *Владельца сертификата* не имеется.

От *Агента*

_____/_____
(Подпись)

_____
(Дата подписи)

М.П.

От *Владельца сертификата*

_____/_____
(Подпись)

_____
(Дата подписи)

АКТ ПРИЕМА – ПЕРЕДАЧИ *СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ*

<Город> <Дата создания акта>

Юридическое лицо < наименование организации, введенное при выдаче *Сертификата* >, именуемое в дальнейшем " *Владелец сертификата* ", представленное своим уполномоченным лицом <ФИО уполномоченного лица, оформившего заявку на сертификат> , с одной стороны, и <Наименование *Агента* >, именуемое в дальнейшем «*Агент*», в лице < должность и ФИО уполномоченного сотрудника Банка >, действующ(-его)(-ей) на основании <документ>, с другой стороны, в соответствии с Правилами работы *Удостоверяющего центра* ЦЦС «BeSafe.ru», составили настоящий Акт приема - передачи о следующем:

1. *Агент* произвел проверку данных *Клиента*, *Удостоверяющий центр* осуществил изготовление *Сертификата ключа проверки электронной подписи (далее – «Сертификат»)* и передал ДД.ММ.ГГГГ *Сертификат Владельцу сертификата*, а *Владелец сертификата* принял оригинал следующего *Сертификата* на *Ключевой носитель*:

Идентификатор *Владельца сертификата*	CN= , OU= , O= , L= , C=
Номер *Сертификата*	
Алгоритм подписи	
Заверен	
Годен с	
Годен до	
Алгоритм *Ключа проверки электронной подписи*	
Ключ проверки электронной подписи	
Алгоритм отпечатка	
Отпечаток	

2. Обязательства *Агента* перед *Владельцем сертификата* выполнены в точном соответствии с Правилами работы *Удостоверяющего центра* ЦЦС «BeSafe.ru», претензий у *Владельца сертификата* не имеется.

От *Агента*	От *Владельца сертификата*
_____/_____	_____/_____
(Подпись)	(Подпись)
_____	_____
(Дата подписи)	(Дата подписи)
М.П.	М.П. (если применимо)

Директору ЗАО «ЦЦС»
От _____

Заявка на поставку Смарт-ключей

Просим осуществить поставку Смарт-ключей и их предперсонализацию в рамках Сервиса «FAKTURA.RU» корпоративной информационной Системы «BeSafe» в следующем количестве:

Наименование Смарт-ключа	Количество, шт.

Представитель Агента:	_____ (Фамилия, Имя, Отчество)
Информация об Агенте:	_____ (наименование)
	_____ (Ф.И.О. ответственного лица, номер мобильного телефона для контактов, e-mail)
	_____ (почтовый адрес для доставки карт)

Подписано От Агента
_____ (_____)
М.п.