Утверждаю:
Директор
Закрытого акционерного общества «Центр Цифровых Сертификатов»

_____ М.М. Муканова

«04» августа 2015 г.

Правила работы Удостоверяющего центра «AUTHORITY»

Правила вступают в силу с «01» сентября 2015 г.

Статья 1. Положение о работе Удостоверяющего центра

1.1. *Удостоверяющий центр* «AUTHORITY» – удостоверяющий центр, созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ЗАО «ЦЦС»), который осуществляет изготовление *Сертификатов ключа проверки электронной подписи* для юридических и физических лиц для возможности осуществления *Электронного документооборота* в рамках корпоративной информационной *Системы «BeSafe»* (далее – «*Система»*).

1.2. Далее по тексту настоящих Правил *Удостоверяющий центр* «AUTHORITY» ЗАО «ЦЦС» именуется как *Удостоверяющий центр (УЦ)*.

1.3. Настоящие Правила определяют порядок и условия изготовления, распространения *Сертификатов* и прекращения срока их действия.

Статья 2. Термины и определения

Система «BeSafe» (далее – «Система») – корпоративная информационная система, представляющая собой совокупность программного, информационного и аппаратного обеспечения. Правила *Системы* размещены в сети Интернет по адресу www.besafe.ru.

Удостоверяющий центр (УЦ) – юридическое лицо, указанное в п. 1.1. настоящих Правил, осуществляющее изготовление *Сертификатов* и *Технологических сертификатов Клиентов*. *УЦ* или уполномоченные им представители (*Агенты*) осуществляют проверку *Клиентов* и документов *Клиентов*, необходимых для создания *Сертификатов* и *Технологических сертификатов Клиента*.

Агент (Доверенное лицо) – уполномоченный представитель *УЦ*, присоединившийся к Правилам *УЦ* посредством Соглашения, заключенного по форме Приложения № 1 к настоящим Правилам. *Агент* осуществляет от имени *УЦ* проверку *Клиентов*, документов *Клиентов*, предшествующую изготовлению *УЦ Сертификатов* и *Технологических сертификатов*, а также направляет *УЦ* запросы на изготовление *Сертификата* или *Технологического сертификата* и передает *Клиенту Сертификат* или *Технологический сертификат*, изготовленный *УЦ*. *Агент* в случае необходимости осуществляет выдачу *Клиентам Ключевых носителей*, содержащих *Криптографические ключи*, *Сертификаты* или *Технологические Сертификаты*, изготовленные *УЦ*, в порядке, предусмотренном настоящими Правилами.

Клиент – физическое лицо (в том числе индивидуальный предприниматель) или юридическое лицо.

Участник – *УЦ*, *Агент* или *Клиент* в соответствии с настоящими Правилами.

Усиленная неквалифицированная электронная подпись (Электронная подпись, ЭП, Электронная цифровая подпись, ЭЦП) – реквизит *ЭД*, предназначенный для защиты *ЭД* от подделки, полученный в результате криптографического преобразования информации с использованием *Ключа ЭП* и позволяющий идентифицировать *Владельца сертификата*, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в *ЭД* информации.

Электронное сообщение (ЭС) – логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия. Информация в *Электронном сообщении* представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

Электронный документ (ЭД) – *Электронное сообщение*, заверенное *ЭП*, в котором информация представлена в электронно-цифровой форме и соответствует установленному в рамках *Системы* формату. *ЭД* может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

Формат электронного документа (Формат ЭД) – структура содержательной части *Электронного сообщения*, на основе которого сформирован *ЭД*.

Отправитель электронного документа (Отправитель ЭД) – *Участник*, который направляет *ЭД* с использованием *Системы*.

Получатель электронного документа (Получатель ЭД) – *Участник*, которому *ЭД* отправлен с использованием *Системы*.

Доставка электронного документа (Доставка ЭД) – процесс пересылки *ЭД* от *Отправителя ЭД* к *Получателю ЭД*.

Электронный документооборот (ЭДО) – обмен *ЭД* в *Системе* в соответствии с настоящими Правилами.

Ключ электронной подписи (Ключ ЭП, Закрытый (секретный) ключ ЭП, Закрытый (секретный ключ электронной подписи) - последовательность символов, известная *Владельцу сертификата* и предназначенная для создания в *ЭД Электронной подписи* с использованием *Средств ЭП*, а также расшифровывания *Электронных сообщений*.

Ключ проверки электронной подписи (Ключ проверки ЭП, Открытый ключ ЭП, Открытый ключ электронной подписи) - последовательность символов, соответствующая *Ключу ЭП*, предназначенная для подтверждения (проверки) с использованием *Средств ЭП* подлинности *ЭП* в *ЭД*, а также зашифровывания *Электронных сообщений*, предназначенных владельцу *Ключа ЭП*.

Криптографические ключи – общее название *Ключей ЭП и Ключей проверки ЭП*.

Ключевая пара – *Ключ ЭП и Ключ проверки ЭП*, однозначно соответствующие друг другу.

Сертификат ключа проверки электронной подписи (Сертификат, Сертификат ключа проверки ЭП, Сертификат ключа электронной подписи) – *ЭД* или документ на бумажном носителе с *ЭП УЦ*, доступный любому *Участнику*, включающий в себя *Ключ проверки ЭП*. *Сертификаты* выдаются УЦ *Участнику* для подтверждения подлинности *ЭП* и идентификации *Владельца сертификата*, а также для обеспечения возможности шифрования предназначенных владельцу *Ключа ЭП Электронных сообщений*. *Сертификат* уникален в рамках выдавшего его *УЦ*.

Технологический сертификат – общее название *Сертификатов,* не используемых для юридически значимого документооборота в рамках *Системы*. Использование *Технологических сертификатов* не регулируется правилами *Системы*.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного *Электронного сообщения.*

Средства криптографической защиты информации (СКЗИ) – аппаратные и(или) программные средства, обеспечивающие применение *ЭП* и *шифрования* при организации *ЭДО*. *СКЗИ* могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение. В *Системе* допускается использование только *СКЗИ*, разрешенных к использованию в *Системе*.

Средства электронной подписи (Средства ЭП) - аппаратные и(или) программные средства, являющиеся частью *СКЗИ* и реализующие хотя бы одну из следующих функций при организации *ЭДО*: создание *ЭП* в *ЭД* с использованием *Ключа ЭП*; подтверждение подлинности *ЭП,* содержащейся в *ЭД*, с использованием *Ключа проверки ЭП*; создание *Ключей ЭП* и *Ключей проверки ЭП*.

Подтверждение подлинности Электронной подписи в Электронном документе (Проверка ЭП документа, Проверка электронной подписи документа) - положительный результат проверки принадлежности *ЭП* в *ЭД Участнику* и отсутствия искажений в данном *ЭД*. Подтверждение подлинности *ЭП* должно осуществляться соответствующим средством *ЭП* с использованием *Сертификата*.

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата ключа проверки электронной подписи, Владелец сертификата) – физическое, либо юридическое лицо (в лице уполномоченного представителя), которому *УЦ* выдан *Сертификат* и которое владеет соответствующим *Ключом ЭП,* позволяющим с помощью *СКЗИ* создавать *ЭП* в *ЭД* (подписывать *ЭД*), а также расшифровывать *Электронные сообщения*.

Идентификатор владельца сертификата ключа проверки электронной подписи (Идентификатор владельца сертификата) – идентификационные данные *Владельца сертификата*, которые входят в состав *Сертификата*. *Идентификатор владельца сертификата* позволяет отличать и однозначно идентифицировать *Владельца сертификата* в рамках *Системы*. *Идентификаторы владельцев сертификатов* одного *Класса*, принадлежащие разным *Владельцам сертификатов*, уникальны в рамках

выдавшего *Сертификаты УЦ*. Уникальность *Идентификаторов владельцев сертификатов* одного *Класса*, принадлежащих разным *Владельцам сертификатов*, обеспечена технологическими средствами *УЦ* при условии, что *Владелец сертификата* не допустил *Компрометации* собственных *Ключей ЭП*.

Класс сертификата ключа проверки электронной подписи (Класс) – атрибут *Сертификата*, характеризующий процедуру проверки, которую прошел *Владелец сертификата* при создании *Сертификата*.

Создание сертификата ключа проверки электронной подписи (Создание сертификата) – осуществляемая *УЦ* процедура изготовления, выдачи и занесения в реестр *Сертификата*.

Компрометация ключа электронной подписи (Компрометация ключа ЭП) – нарушение конфиденциальности *Ключа ЭП*, констатация *Владельцем сертификата* обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование *Ключа ЭП* неуполномоченными лицами.

Уполномоченное лицо участника – сотрудник или иной представитель *Участника*, действующий от его имени на основании Устава, договора, доверенности на право совершения соответствующих операций.

Ключевой носитель – информационный (материальный) носитель, на который записаны *Криптографические ключи*.

Смарт-ключ - компактное программно-аппаратное устройство, предназначенное для хранения *Ключа проверки ЭП, Ключа ЭП, Сертификата*, а также другой электронно-цифровой информации. *Смарт-ключ* имеет защищенную память, где создаются и в последующем сохраняются секретные ключи ЭП. Чтение или копирование секретных ключей ЭП из защищенной памяти *Смарт-ключа* невозможно.

Статья 3. Правовое регулирование отношений в области использования Сертификатов

3.1. Правовое регулирование отношений в области использования *Сертификатов УЦ* осуществляется в соответствии с Федеральным законом от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» (в части, касающейся деятельности *Системы*), Гражданским Кодексом РФ, Правилами *Системы*, настоящими Правилами, а также, при необходимости, дополнительными договорами и соглашениями *Участников ЭДО*.

3.2. Во всем, что не урегулировано настоящими Правилами, Правилами *Системы*, а также договорами и соглашениями *Участников ЭДО* (при их наличии), *Участники* руководствуются действующим законодательством Российской Федерации.

3.3. Описание атрибутов *Сертификатов*, позволяющее отнести *Сертификат*, выданный *УЦ*, к какому-либо *Классу*, либо признать его *Технологическим сертификатом*, приведено в Приложении № 9 к настоящим Правилам.

3.4. *Сертификаты Классов* 2, 3 и 4, изготовленные *УЦ* в порядке и на условиях настоящих Правил, предназначены для обеспечения *ЭДО* исключительно в рамках Правил *Системы*.

3.5. *Технологические сертификаты* не предназначены для использования в качестве *Сертификатов* в рамках правил *Системы*.

Статья 4. Деятельность Удостоверяющего центра

4.1. *УЦ* изготавливает *Сертификаты* и *Технологические сертификаты* в форме *ЭД*, устанавливает сроки действия *Сертификатов*, *Технологических Сертификатов* и предоставляет возможность получения копий *Сертификатов* и *Технологических Сертификатов* в виде документов на бумажных носителях. *УЦ* может изготавливать *Ключевые носители*, содержащие *Ключи ЭП*, *Сертификаты*, которые после осуществления предусмотренных Правилами процедур, позволяют формировать *ЭП*.

4.2. *УЦ* ведет реестр *Сертификатов* и *Технологических сертификатов*, обеспечивает его актуальность и возможность доступа к нему участников информационных систем. *Сертификаты* и *Технологические сертификаты*, созданные *Удостоверяющим центром*, подлежат внесению *Удостоверяющим центром* в реестр *Сертификатов* и *Технологических сертификатов* не позднее даты начала действия *Сертификата* и *Технологического сертификата*.

4.3. *УЦ* также может выполнять функции *Агента*, предусмотренные Статьями 7, 8, 9 настоящих Правил.

4.4. Срок действия *Сертификата Класса* 2,3,4 составляет один год с момента его создания *Удостоверяющим центром*.

4.5. *УЦ* не несет ответственности за любые убытки, которые могут возникнуть у *Клиентов*, *Владельцев сертификатов* и иных лиц в связи с использованием *Сертификатов*, *Технологических сертификатов*, *Криптографических ключей*, в том числе убытки, связанные с неправомочным использованием. Все риски, связанные с использованием *Сертификатов*, *Технологических сертификатов*, *Криптографических ключей* несут *Клиент*ы, *Владельцы сертификатов*.
4.6. *УЦ* проверяет уникальность *Ключей проверки ЭП* в реестре *Сертификатов* и *Технологических сертификатов*;
4.7. *УЦ* осуществляет по обращениям *Участников* электронного взаимодействия проверку *ЭП*;
4.8. *УЦ* осуществляет иную связанную с использованием *ЭП* деятельность.

Статья 5. Порядок создания Технологических сертификатов

5.1. Порядок изготовления *Технологических сертификатов* определяется для каждого *Клиента* отдельным соглашением между *УЦ* и *Клиентом*.

Статья 6. Общие положения создания Сертификатов

6.1. Изготовление *Сертификатов* осуществляется на основании Заявления *Клиента*, поданного им *Агенту*. Заявление содержит сведения, необходимые для проверки информации о *Клиенте* в соответствии с *Классом* запрашиваемого *Клиентом Сертификата* и передачи *Клиенту* сообщений. Заявление формируется в соответствии с типовой формой (Приложение №5 для *Клиента* - физического лица; Приложение №6 для *Клиента* – юридического лица) и подписывается собственноручно *Клиентом* или его уполномоченным лицом. Содержащиеся в Заявлении сведения подтверждаются предъявлением соответствующих документов (для физических лиц – паспорт, для представителей юридических лиц – паспорт, а также письменный документ, заверенный подписью руководителя и печатью организации, подтверждающий право представителя действовать от имени данной организации). Проверку предоставленных *Клиентом* сведений производит *Агент*. Проверка производится в соответствии с *Классом сертификата*. По требованию *УЦ Агент* обязан направить в *УЦ* заверенную копию Заявления *Клиента* с отметкой *Агента* о его принятии, а также заверенные копии документов, представленных *Клиентом Агенту*. Направление заверенной копии осуществляется *Агентом* за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от *УЦ*. В случае не направления вышеуказанного Заявления и документов в предусмотренный срок, *УЦ* вправе приостановить деятельность такого *Агента* по формированию запросов на создание *Сертификатов* и их выдачи *Клиентам*, письменно уведомив об этом *Агента*.

6.2. При изменении данных, идентифицирующих *Владельца сертификата*, содержащихся в документах, предоставленных при выдаче *Сертификата*, смене *Криптографических ключей*, в случаях *Компрометации ключей*, *Владельцу сертификата* надлежит получить новый *Сертификат* в порядке, предусмотренном настоящей статьей. Все риски, связанные с невозможностью использования *Сертификата* в связи с изменением данных, идентифицирующих *Владельца сертификата*, несет *Владелец сертификата*.

6.3. В случае если *Владелец сертификата* обладает действующим (не утратившим силу) *Сертификатом*, возможно создание нового *Сертификата* по удаленному обращению *Владельца сертификата* в порядке, определенном Статьей 9 настоящих Правил.

6.4. Возможен иной порядок выдачи *Сертификатов*, определённый *УЦ*.

6.5. При возникновении технического сбоя передачи и/или обработки запроса на выдачу *Сертификата*, в результате которого *Агент / Клиент Агента* не получил запрошенный *Сертификат, Агент* отправляет Заявление в форме ЭД согласно Приложению №4 к Правилам (Заявление на сбойные Сертификаты). *Сертификат* признается сбойным, если заявление на объявление его сбойным приходит в течение отчетного месяца, в котором произошел технический сбой.

6.6. В случае если в течение отчетного месяца возникновения технического сбоя от *Агента* не поступит запрос в виде электронного документа на объявление *Сертификата* сбойным, то такой *Сертификат* признается *Сертификатом* надлежащего качества, полученным *Агентом*, и подлежит оплате в соответствии с условиями настоящих Правил.

Статья 7. Порядок создания Сертификатов с генерацией Ключевой пары Клиентом

7.1. Изготовление *Ключевой пары* и запроса на выдачу *Сертификата* осуществляется *Клиент*ом самостоятельно на своем персональном компьютере. Для этого *Клиент*, при необходимости, устанавливает требуемое программное обеспечение, заходит по ссылке, предоставленной *Агентом*, заполняет отображаемую форму Заявления на создание *Сертификата* и отправляет запрос. Запрос формируется в виде *ЭД* и направляется в *УЦ* с использованием программно-аппаратных средств *Клиента*, подключенных через каналы связи к программно-техническим средствам *УЦ*. Запрос содержит *Ключ проверки ЭП*, а также уникальный *Идентификатор владельца сертификата* (DN), сформированный на основе данных *Клиента*.

7.2. При изготовлении *Сертификатов* всегда проверяется уникальность *Идентификаторов владельцев сертификатов* (DN), принадлежащих разным *Владельцам сертификатов,* в реестре и архиве *УЦ*. Программно-аппаратные средства *УЦ* исключают возможность создания двух *Сертификатов* с совпадающими *Идентификаторами владельцев сертификатов*, принадлежащих разным *Владельцам сертификатов*, при условии, что *Ключи ЭП* не были скомпрометированы. В случае успешной проверки на уникальность *УЦ* отображает страницу, содержащую уникальный номер запроса (УНЗ), а также предложение распечатать Заявление на выдачу *Сертификата*. *Клиенту* необходимо сохранить УНЗ для последующего обращения к *Агенту УЦ*.

7.3. *Клиент* обращается к *Агенту*, сообщает УНЗ и предоставляет необходимые документы в соответствии с пунктом 6.1. Получив Заявление, подписанное *Клиентом*, и проверив данные *Клиента* в соответствии с пунктом 6.1., *Агент* подтверждает запрос на создание *Сертификата*. Подтверждение запроса на выдачу *Сертификата Клиента* формируется в виде *ЭД*, подписанного *ЭП Агента* и направляется *в УЦ* с использованием программно-аппаратных средств *Агента*, подключенных через каналы связи к программно-техническим средствам *УЦ*.

7.4. Создание *Сертификатов* для *Агента*/*Клиентов* осуществляется *Удостоверяющим центром* в течение 3 (Трех) рабочих дней с момента получения от *Агента* подтверждения запроса в соответствии с п. 7.3.

7.5. *Агент* распечатывает на бумажном носителе Акт приема-передачи *Сертификата Клиента* согласно Приложению №7 для *Клиента* - физического лица и Приложению №8 для *Клиента* – юридического лица в двух экземплярах и обеспечивает проставление в них собственноручной подписи *Клиента* или уполномоченного лица *Клиента*. Второй экземпляр Акта приема-передачи на бумажном носителе хранится у *Агента*. По требованию *УЦ Агент* обязан направить *Удостоверяющему центру* заверенную копию Акта. Направление заверенной копии осуществляется *Агентом* за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от *УЦ*. В случае не направления вышеуказанного Акта в предусмотренный срок, *УЦ* вправе приостановить деятельность такого *Агента* по формированию запросов на создание *Сертификатов* и их выдачи *Клиентам*, письменно уведомив об этом *Агента*.

7.6. *УЦ* отправляет *Клиенту* на указанный в Заявлении на выдачу *Сертификата* адрес электронной почты ссылку для сохранения *Сертификата*, созданного по подтвержденному *Агентом* запросу *Клиента*.

Статья 8. Порядок создания Сертификатов с генерацией Ключевой пары Агентом

8.1. Получив Заявление и проверив данные *Клиента* в соответствии с п.6.1, *Агент* формирует запрос на создание *Сертификата*. Запрос формируется в виде *ЭД*, подписанного *ЭП Агента* и направляется *в УЦ* с использованием программно-аппаратных средств *Агента*, подключенных через каналы связи к программно-техническим средствам *УЦ*. Запрос содержит *Ключ проверки ЭП*, а также уникальный *Идентификатор владельца сертификата* (DN), сформированный на основе проверенных *Агентом* данных *Клиента*.

8.2. Создание *Сертификатов* для *Агента*/*Клиентов* осуществляется *УЦ* в течение 3 (Трех) рабочих дней с момента получения от *Агента* электронного запроса в соответствии с п. 8.1. Передача *УЦ* или уполномоченными им лицами *Агенту Ключевых носителей*, содержащих *Ключ ЭП* и *Сертификат*, созданных *УЦ* без получения Заявления от *Клиента*, осуществляется в порядке и на условиях, определяемых *УЦ* и *Агентом* дополнительно.

8.3. При изготовлении *Сертификатов* всегда проверяется уникальность *Идентификаторов владельцев сертификатов* (DN), принадлежащих разным *Владельцам сертификатов*, и *Ключей проверки ЭП* в реестре и архиве *УЦ*. Программно-аппаратные средства *УЦ* исключают возможность изготовления одинаковых *Сертификатов*. При изготовлении *Ключевых носителей*, *УЦ* самостоятельно формирует уникальный *Идентификатор владельца сертификата* (DN) и присваивает его созданному *Сертификату*.

8.4. *УЦ* предоставляет *Агенту* созданные по Заявлению/запросу *Агента Сертификаты* для *Агента*/*Клиентов* в форме *ЭД*.

8.5. *Агент* при выдаче *Криптографических ключей Клиента* распечатывает на бумажном носителе Акт приема-передачи *Сертификата Клиента* согласно Приложению №7 для *Клиента* - физического лица и Приложению №8 для *Клиента* – юридического лица в двух экземплярах и обеспечивает проставление в них собственноручной подписи *Клиента* или уполномоченного лица *Клиента*. Второй экземпляр Акта приема-передачи на бумажном носителе хранится у *Агента*. По требованию *УЦ Агент* обязан направить *в УЦ* заверенную копию Акта. Направление заверенной копии осуществляется *Агентом* за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от *УЦ*. В случае не направления вышеуказанного Акта в предусмотренный срок, *УЦ* вправе приостановить деятельность такого *Агента* по формированию запросов на создание *Сертификатов* и их выдачи *Клиентам,* письменно уведомив об этом *Агента*.

Статья 9. Порядок создания Сертификатов по удаленному обращению Клиента, уже являющегося Владельцем сертификата

9.1. *Клиент* обращается на страницу сервера *УЦ*, предназначенную для удаленной выдачи *Сертификатов*, при этом:

9.1.1. *Клиент*, уже являющийся *Владельцем сертификата УЦ*, срок действия которого не истек, формирует новую пару *Ключа ЭП* и *Ключа проверки ЭП*, а также запрос на новый *Сертификат*.

9.1.2. *Клиент* подписывает запрос на новый *Сертификат* действующим *Ключом ЭП*. *Идентификаторы владельца сертификата* нового и действующего *Сертификата* должны совпадать.

9.1.3. *Клиент* передает заверенный действующим *Ключом ЭП* запрос на новый *Сертификат* серверу *УЦ*. Запрос равнозначен Заявлению *Клиента* на выдачу *Сертификата*, заверенному собственноручной подписью *Клиента* или уполномоченного лица *Клиента*.

9.2. *Агент* обращается на сервер *УЦ* и подтверждает выдачу нового *Сертификата Клиента*.

9.3. *УЦ* изготавливает новый *Сертификат* по запросу *Клиента*. *Класс* нового *Сертификата* совпадает с *Классом* действующего *Сертификата Клиента*.

9.4. *Агент* обращается на сервер *УЦ* и получает Акт приема-передачи нового *Сертификата Клиента*.

9.5. *Агент* заверяет Акт приема-передачи нового *Сертификата Клиента Электронной подписью* и передает его *Удостоверяющему центру*, подтверждая тем самым выдачу нового *Сертификата Клиенту*.

9.6. *Агент* или *УЦ* сообщает *Клиенту* адрес выдачи нового *Сертификата*.

9.7. *Клиент* обращается по указанному адресу, получает заверенный *Агентом* Акт приема-передачи нового *Сертификата*.

9.8. *Клиент* заверяет действующей *ЭП* Акт приема-передачи нового *Сертификата* и передает Акт в *УЦ*.

9.9. *Клиент* получает новый *Сертификат*.

9.10. *Сертификат* помещается в реестр *Сертификатов*.

9.11. Так как Акт приема-передачи формируется в электронном виде и сохраняется *УЦ*, *Агент* может в этом случае Акт не хранить.

9.12. *Агент* может отказаться от подтверждения выдачи нового *Сертификата Клиента*, при этом *Агент* или *УЦ* направляет *Клиенту* сообщение об отказе.

Статья 10. Условия оплаты Агентом вознаграждения Удостоверяющего центра

10.1. Размер, виды и периодичность выплаты вознаграждения определяются *УЦ* и размещаются для ознакомления в сети Интернет по адресу bank.faktura.ru. Доступ к информации предоставляется по заявке, направляемой по электронной почте на адрес support@faktura.ru.

10.2. Основанием для оплаты является счет, выставляемый *УЦ Агенту*. Оплата в соответствии с настоящим разделом осуществляется *Агентом* в течение 5 (Пяти) рабочих дней с момента получения *Агентом* счета от *УЦ*.

Статья 11. Срок и порядок хранения Сертификатов и Технологических сертификатов в Удостоверяющем центре

11.1. Срок хранения *Сертификатов* в *УЦ* после прекращения действия определяется законодательством.

11.2. По истечении указанного срока хранения *Сертификат* исключается из реестра и переводится в режим архивного хранения. Срок архивного хранения определяется Правилами *Системы*.

11.3. Срок хранения *Технологических сертификатов* в *УЦ* определяется соглашением с *Клиентом*.

Статья 12. Права и обязанности Удостоверяющего центра

12.1. *УЦ*, проводя изготовление *Сертификата*, принимает на себя следующие обязанности по отношению к *Владельцу сертификата*:
- внести *Сертификат* в реестр *Сертификатов*.
- осуществлять проверку данных *Клиента* для удостоверения *Ключей проверки ЭП* в соответствии с правилами определенного *Класса Сертификата*;
- обеспечивать выдачу *Сертификата* обратившимся к нему *Клиентам Системы*;

12.2. *УЦ* вправе отказать *Клиенту* в изготовлении *Сертификата* в случае, если проверка данных *Клиента* не подтвердила их достоверность, либо *Идентификатор владельца сертификата* (DN) оказался не уникальным, либо если *Клиент* не является участником *Системы*.

12.3. *УЦ* обязан в максимально сжатые сроки уведомлять *Агента* об ошибках, возникающих в работе программно-технических средств *УЦ* (в том числе в связи с попытками нарушения информационной безопасности), которые могут повлечь нарушения в обмене *ЭД* и непосредственно повлиять на работу *Агента* и/или его *Клиентов*.

12.4. УЦ имеет право временно приостановить действие выданных *Агентом Сертификатов Клиентов Агента* в случае обнаружения факта несоответствия указанных в запросе реквизитов фактическим данным до устранения таких несоответствий, внесения соответствующих изменений.

12.5. В случае просрочки оплаты вознаграждения *УЦ*, предусмотренного Правилами, *УЦ* вправе взыскать с *Агента* неустойку в размере 0,1% от неоплаченной суммы за каждый день просрочки.

Статья 13. Права и обязанности Агента

13.1. *Агент* обязан за свой счет сформировать программно-аппаратные комплексы и обеспечивать каналы связи, необходимые для доступа к программно-техническим средствам *УЦ* для получения *Сертификатов*.

13.2. *Агент* обязан производить проверку соответствия сведений, содержащихся в заявлениях *Клиентов Агента*, документам *Клиента* (в соответствии с п. 6.1 Настоящих Правил). *Агент* несет ответственность перед *УЦ*, третьими лицами за достоверность данных, указанных в сформированном и/или подтвержденном им запросе на создание *Сертификата Клиента Агента*, а также за обеспечение выдачи *Клиентам Агента* надлежащим образом оформленных *Сертификатов.*

13.3. *Агент* обязан хранить Заявления *Клиента* и Акты приема-передачи в течение всего срока работы в качестве *Агента*. По запросу *УЦ*, а также при выходе из статуса *Агента, Агент* обязан в течение 15 календарных дней передать Заявления *Клиента* и Акты приема-передачи в *УЦ*. При несоблюдении обязательств настоящего пункта Агент обязан по письменному требованию УЦ возместить все возникшие ввиду этого документально подтвержденные убытки УЦ.

13.4. *Агент* обязан информировать *УЦ* о компрометации, аннулировании, прекращении действия *Сертификата Агента* и *Клиентов Агента* по иным основаниям, направив соответствующее уведомление.

13.5. *Агент* обязан регулярно знакомиться с изменениями в настоящих Правилах, публикуемых в сети Интернет по адресу www.authority.ru.

Статья 14. Права и обязанности Владельца сертификата

14.1. *Владелец сертификата* обязан:
- использовать только собственные уникальные *Ключи ЭП*;
- хранить в тайне *Ключи ЭП*;
- требовать приостановления действия *Сертификата* в корпоративной финансовой, информационной или иной системе при наличии подозрений на *Компрометацию ключа ЭП* в максимально сжатые сроки;

14.2. Под *Компрометацией* (нарушением конфиденциальности) *Ключей ЭП* понимается утрата доверия к тому, что используемые *Ключи ЭП* недоступны третьим лицам. К событиям, связанным с *Компрометацией ключей* относятся следующие события:
- утрата *Ключевых носителей*;
- утрата *Ключевых носителей* с последующим обнаружением;
- увольнение сотрудников, имевших доступ к *Ключам ЭП*;

- утрата ключей от сейфа, хранилища в момент нахождения в нем *Ключевых носителей*;
- иные обстоятельства прямо или косвенно свидетельствующие о наличии возможности доступа к *Ключу ЭП* третьих или неуполномоченных лиц.

14.3. *Владелец сертификата* регулярно знакомится с информацией об изменениях в Правилах, размещаемой *Удостоверяющим центром* по адресу www.authority.ru.

Статья 15. Порядок внесения изменений в настоящие Правила и Тарифы УЦ

15.1. *УЦ* имеет право в одностороннем порядке менять настоящие Правила, разместив новую редакцию Правил по адресу www.authority.ru за 14 (Четырнадцать) календарных дней до вступления новых правил в силу.

15.2. *УЦ* имеет право изменять Тарифы и условия оплаты вознаграждения в сроки, аналогичные п. 15.1 настоящих Правил, разместив новые тарифы по адресу bank.faktura.ru. В случае, когда изменение Тарифов вызвано изменением стоимости оказания услуг партнеров *УЦ*, допускается сокращение срока размещения Тарифов до 5 (Пяти) календарных дней до даты их вступления в силу.

Статья 16. Конфиденциальность и персональные данные

16.1. *УЦ* и *Агент* принимают на себя обязательства рассматривать всю информацию, полученную в ходе взаимодействия на условиях Правил (в том числе о размерах и условиях уплаты вознаграждения *Агента*), как конфиденциальную, не подлежащую разглашению, и отвечают за соблюдение данного требования.

16.2. *УЦ* обеспечивает безопасное хранение используемой информации, и предоставляет доступ к ней только уполномоченным лицам.

16.3. *УЦ* обеспечивает конфиденциальность персональных данных, обрабатываемых в *УЦ*, соответствии с действующим законодательством.

16.3.1. *Ключ ЭП* является конфиденциальной информацией *Владельца сертификата*. *УЦ* не осуществляет хранение *Ключей ЭП*.

16.3.2. Информация о *Владельцах сертификатов*, не подлежащая непосредственной рассылке в качестве части *Сертификата*, является конфиденциальной.

16.3.3. Информация, включаемая в *Сертификаты*, издаваемые *УЦ*, в том числе персональные данные, не считается конфиденциальной.

16.3.4. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

16.3.5. Открытая информация может публиковаться по решению *УЦ*. Место, способ и время публикации открытой информации определяется *УЦ*.

16.4. *УЦ* и *Агент* соглашаются, что обеспечение *УЦ* взаимодействия на условиях Правил не нарушает прав собственности *Агента*, *Клиентов Агента* в отношении передаваемой информации, а также не нарушает обязательств по неразглашению информации со стороны *Агентов*.

16.5. Действие настоящего раздела не распространяется на случаи, когда передача информации третьим лицам необходима для выполнения условий настоящих Правил, а также случаи, предусмотренные действующим законодательством Российской Федерации.

Статья 17. Дополнительные условия

17.1. Особенности взаимодействия *УЦ* и *Агента* по вопросам создания *Сертификатов* для нужд *Агента* и поставки *Смарт-ключей Агенту* описаны в Приложении №2 к настоящим Правилам.

17.2. *Агент* вправе расторгнуть отношения с *УЦ* в рамках настоящих Правил в одностороннем внесудебном порядке путем направления *УЦ* письменного уведомления не менее чем за 30 (Тридцать) дней до предстоящей даты расторжения.

17.3. Обязательства *Агента*, возникшие до момента прекращения отношений в рамках настоящих Правил по любым основаниям, подлежат исполнению в полном объеме и в соответствии с условиями Правил.

17.4. В случае просрочки оплаты *Агентом* денежных средств, предусмотренных п.10.2 Правил, более 30 (Тридцати) дней, *УЦ* вправе в одностороннем порядке приостановить исполнение своих обязательств, предусмотренных настоящими Правилами, до погашения *Агентом* в полном объеме задолженности, включая штрафные санкции.

17.5. Разногласия, возникшие между *УЦ* и *Агентом* при исполнении положений настоящих Правил, разрешаются путем переговоров. В противном случае неразрешенные споры передаются на рассмотрение в Арбитражный суд Новосибирской области в соответствии с действующим законодательством Российской Федерации.

Статья 18. Переходные положения

18.1. В соответствии с условиями Договоров с *УЦ*, заключенных *Агентами* после 01 апреля 2008 года, положения настоящих Правил имеют приоритет над условиями Договоров.

СОГЛАШЕНИЕ № _____
О ПРИСОЕДИНЕНИИ К ПРАВИЛАМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА «AUTHORITY»

«___» _____20__ года

г. Новосибирск

Закрытое акционерное общество «Центр Цифровых Сертификатов», именуемое в дальнейшем «Удостоверяющий центр», в лице Директора Мукановой Мадины Мукаметракимовны, действующей 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 «AUTHORITY.RU», которые расположены в Интернете по адресу www.authority.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 www.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 / ФИЛИАЛ АГЕНТА**
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.М. Муканова)	_____ (_____)
М.п.	М.п.

Особенности создания Сертификатов для нужд Агентов

1. *УЦ* 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 УЦ*.
2. После получения *Сертификата Агент* обязан направить в *УЦ* 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 *УЦ Агенту Сертификата*, *УЦ* и *Агент* подписывают Акт приема-передачи по форме, указанной в Приложении №8 к Правилам.

Порядок поставки Удостоверяющим центром Смарт-ключей Агенту

1. *УЦ* предоставляет *Агенту Смарт-ключи* в качестве средства хранения *Ключей ЭП*, Сертификатов.
2. Количество *Смарт-ключей*, подлежащих поставке *УЦ Агенту*, определяется в заявлении, направляемом *Агентом в УЦ*. На основании полученного заявления *Агента, УЦ* выставляет *Агенту* счет на оплату. Заявление на поставку *Смарт-ключей*, а также их предперсонализацию, направляются *Агентом* в *УЦ* в электронном (сканированном) виде по адресу market@faktura.ru. Форма заявления приведена в Приложении №10 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 *УЦ* 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 *УЦ*.
7. Создание *Сертификата*, передача его *Агенту* для последующей записи на *Смарт-ключ* осуществляется *УЦ* 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 «AUTHORITY»
Заявление для УЦ от Агента на регистрацию прав сотрудников

Директору ЗАО «ЦЦС»
Мукановой М.М.
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 Ключей 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 Ключей с правом подписывать акты приема-передачи Сертификатов клиентам.

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

____ _____20___года

_____(должность, реквизиты доверенности)

_____ /_____/
(Ф.И.О.)

М.П.

Директору ЗАО «ЦЦС»
Мукановой М.М.
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	CN=Class 2 CA, O=Center of Financial Technologies, C=RU
2	CN=, OU= , O=, L=, C=RU	CN=Class 2 CA, O=Center of Financial Technologies, 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 «AUTHORITY»
Заявление на выдачу Сертификата (физическое лицо)

Агенту Удостоверяющего центра «AUTHORITY»

<Наименование *Агента*>

/ в Удостоверяющий центр «AUTHORITY»

ЗАЯВЛЕНИЕ НА ВЫДАЧУ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Прошу Удостоверяющий центр «AUTHORITY» изготовить и выдать мне *Сертификат ключа проверки электронной подписи* (*Класс Сертификата*) для физического лица с параметром *Идентификатора владельца сертификата*:_____ (ФИО / псевдоним *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 *Сертификат ключа проверки электронной подписи 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 «AUTHORITY»
Заявление на выдачу Сертификата (юридическое лицо)

Агенту Удостоверяющего центра «AUTHORITY»

<Наименование *Агента*>

/ в Удостоверяющий центр «AUTHORITY»

ЗАЯВЛЕНИЕ НА ВЫДАЧУ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать уполномоченному лицу организации _____(наименование организации), действующ(-ему)(-ей) на основании _____, *Сертификат ключа проверки электронной подписи* (*Класс _ Сертификата*) с параметром *Идентификатора владельца сертификата*:_____ (ФИО \ псевдоним уполномоченного лица организации / наименование \ псевдоним 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 администратора ключей> <Дата создания акта>

<ФИО, введенные при выдаче *Сертификата*>, именуем(-ый)(-ая) в дальнейшем «*Клиент*», с одной стороны, и <Наименование *Агента*> , именуемое в дальнейшем «*Агент*», в лице <должность и ФИО администратора ключей либо иного уполномоченного сотрудника Банка >, действующ(-его)(-ей) на основании <документ >, с другой стороны, в соответствии с Правилами работы *Удостоверяющего центра* «AUTHORITY» 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 Клиенту*, а *Клиент* 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 *Клиентом* выполнены в точном соответствии с Правилами работы *Удостоверяющего центра* «AUTHORITY», претензий у *Клиента* не имеется.

От *Агента*

_____/_____
(Подпись)

_____
(Дата подписи)

М.П.

От *Клиента*

_____/_____
(Подпись)

_____
(Дата подписи)

АКТ ПРИЕМА – ПЕРЕДАЧИ *СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ*

<Город администратора ключей > <Дата создания акта>

Юридическое лицо < наименование организации, введенное при выдаче *Сертификата* >, именуемое в дальнейшем "*Клиент*", 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 администратора ключей либо иного уполномоченного сотрудника Банка >, действующ(-его)(-ей) на основании <документ>, с другой стороны, в соответствии с Правилами работы *Удостоверяющего центра* «AUTHORITY» 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 Клиенту*, а *Клиент* 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 *Клиентом* выполнены в точном соответствии с Правилами работы *Удостоверяющего центра* «AUTHORITY», претензий у *Клиента* не имеется.

От *Агента*

_____/_____
(Подпись)

_____
(Дата подписи)

М.П.

От *Клиента*

_____/_____
(Подпись)

_____
(Дата подписи)

М.П. (если применимо)

Атрибутом *Сертификата ключа проверки электронной подписи (далее – «Сертификат»)*, позволяющим отнести *Сертификат*, выданный *Удостоверяющим центром*, к какому либо *Классу*, либо признать его *Технологическим сертификатом*, является поле со значением *Идентификатора владельца сертификата удостоверяющего центра*, которым подписан данный *Сертификат* или *Технологический сертификат*.

Соответствие Идентификатора *Владельца сертификата ключа проверки электронной подписи Удостоверяющего центра* и *Класса* выданного *Сертификата ключа проверки электронной подписи* по терминологии *Системы*:

Класс Сертификата ключа проверки электронной подписи Системы	Значение *Идентификатора владельца сертификата Удостоверяющего центра*
Класс 2	CN = Class 2 CA O = Center of Financial Technologies C = RU
Класс 3	CN = Class 3 CA O = Center of Financial Technologies C = RU
Класс 4	CN = Class 4 CA O = Center of Financial Technologies C = RU

Значение Идентификаторов *Владельца сертификата Удостоверяющего центра* для *Технологических сертификатов*:

Значение *Идентификатора владельца сертификата Удостоверяющего центра*
CN = Common 1 CA O = Center of Financial Technologies C = RU
CN = Class 1 CA O = Center of Financial Technologies C = RU

Директору ЗАО «ЦЦС»
Мукановой М.М.
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.