УТВЕРЖДАЮ:

Директор ЗАО «ЦЦС»

_____

(Гудков А.В.) М.П

«17» июня 2020 г.

# Правила работы Удостоверяющего центра «AUTHORITY»

Правила вступают в силу с «02» июля 2020 г.

## Статья 1. Положение о работе Удостоверяющего центра

1.1. *Удостоверяющий центр* «AUTHORITY» – удостоверяющий центр, созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ЗАО «ЦЦС»), ОГРН 1025403189602, который осуществляет функции по созданию и выдаче *Технологических сертификатов Клиентов* и *Сертификатов ключей проверки электронных подписей* юридическим и физическим лицам 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 создания и выдачи *Удостоверяющим центром Сертификатов,* сроки действия *Сертификатов* и порядок прекращения срока их действия.

## Статья 2. Термины и определения

2.1. ***Система «BeSafe» (далее – «Система»)*** – корпоративная информационная система, организованная ЗАО «ЦЦС», представляющая собой совокупность программного, информационного и аппаратного обеспечения для обеспечения договорных и технологических условий формирования и развития финансового и информационного электронного обслуживания, предоставляемого ЗАО «ЦЦС» и *Организаторами сервисов Клиентам*. Правила *Системы* размещены в сети Интернет на сайте: www.besafe.ru.

2.2. ***Организатор сервиса*** - *Организатор сервиса*, как определено в Правилах Системы.

2.3. ***Сервис «BeSafe» (далее «Сервис»)*** – часть *Системы «BeSafe»*, предназначенная для финансового и/или информационного электронного обслуживания *Клиентов*.

2.4. ***Удостоверяющий центр (УЦ)*** – юридическое лицо, указанное в п. 1.1 настоящих Правил, осуществляющее создание, выдачу и занесение в реестр *Сертификатов* и *Технологических сертификатов Клиентов*. *УЦ* или уполномоченные им доверенные лица (*Агенты*) осуществляют идентификацию *Клиентов* и проверку документов *Клиентов*, необходимых для создания и выдачи *Сертификатов* и *Технологических сертификатов Клиентам*.

2.5. ***Агент (Доверенное лицо)*** – уполномоченный представитель *УЦ*, присоединившийся к Правилам *УЦ* посредством заключения Соглашения, форма которого определена Приложением № 1 к настоящим Правилам. *Агент* осуществляет от имени *УЦ идентификацию Клиентов*, проверку документов *Клиентов*, предшествующую созданию *УЦ Сертификатов* и *Технологических сертификатов*, а также направляет *УЦ* запросы на создание *Сертификата* или *Технологического сертификата* и передает *Клиенту Сертификат* или *Технологический сертификат*, созданный *УЦ*. *Агент* в случае необходимости осуществляет выдачу *Клиентам Ключевых носителей*, содержащих *Криптографические ключи*, *Сертификаты* или *Технологические Сертификаты*, созданные *УЦ*, в порядке, установленном настоящими Правилами.

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

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

2.8.***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 после момента подписания ЭД.

2.9.***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.

2.10.***Электронный документ (ЭД)*** – *Электронное сообщение*, подписанное *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.

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

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

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

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

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

2.16.***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*.

2.17.***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*.

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

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

2.20.***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*.

2.21.***Технологический сертификат*** – общее название *Сертификатов,* не используемых для юридически значимого документооборота в рамках *Сервиса*. *И*спользование *Технологических сертификатов* не регулируется правилами *Системы, а определяется договорами, заключаемыми между Организаторами Сервисов и УЦ.*

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

2.23.***Средства криптографической защиты информации (СКЗИ)*** – аппаратные и(или) программные средства, обеспечивающие использование *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 тех *СКЗИ*, которые разрешены к использованию в *Системе*.

2.24.***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*.

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

2.26.***Владелец сертификата ключа проверки электронной подписи (Владелец сертификата ключа проверки электронной подписи, Владелец сертификата)*** – физическое, либо юридическое лицо (в лице уполномоченного представителя), которому *УЦ* выдал *Сертификат* и которое владеет соответствующим *Ключом ЭП,* позволяющим с помощью *СКЗИ* создавать *ЭП* в *ЭД* (подписывать *ЭД*), а также расшифровывать *Электронные сообщения.* Допускается не указывать в качестве *Владельца сертификата* физическое лицо, действующее от имени юридического лица, в *Технологическом сертификате*, а также в *Сертификате*, используемом для автоматического создания и (или) автоматической проверки *Электронных подписей* в *Сервисе* только в случаях, предусмотренных Федеральным законом N 63-ФЗ «Об электронной подписи» и другими федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами.

2.27.***Идентификатор владельца сертификата ключа проверки электронной подписи (Идентификатор владельца сертификата, Distinguished Name, DN)*** – идентификационные данные *Владельца сертификата*, которые входят в состав *Сертификата*. Они представляют собой совокупность данных, описываемых в поле сертификата Subject (Субъект) в контексте стандарта x.509 *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* принадлежащих ему *Ключей ЭП*.

2.28.***Класс сертификата ключа проверки электронной подписи (Класс)*** – атрибут *Сертификата*, характеризующий назначение использования *Сертификата*.

2.29.***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. К событиям, связанным с Компрометацией ключей ЭП могут относиться 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.

2.30.***Уполномоченное лицо участника*** – представитель *Участника*, действующий от его имени на основании Устава, доверенности на право совершения соответствующих действий.

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

2.32.***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 *Ключи ЭП*. Чтение или копирование 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. № 63-ФЗ «Об электронной подписи» (в части, касающейся деятельности *Системы*), Гражданским кодексом Российской Федерации, Правилами *Системы*, настоящими Правилами, а также, при необходимости, договорами и соглашениями между *Участниками ЭДО*.

3.2.Во всем, что не урегулировано настоящими Правилами, Правилами *Системы*, Правилами *Сервиса,* а также договорами и соглашениями между *Участниками 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*, указано в Приложении № 9 к настоящим Правилам.

3.4.*Сертификаты Классов* 2, 3 и 4, созданные *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 *Системы*. Технологические сертификаты могут использоваться Участниками для обеспечения дополнительной защиты информации.

**Статья 4. Деятельность Удостоверяющего центра**

4.1.*УЦ* создает *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 предоставлять *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 Системы*. *Сертификаты* и *Технологические сертификаты*, созданные *Удостоверяющим центром*, подлежат внесению *Удостоверяющим центром* в реестр *Сертификатов* и *Технологических сертификатов* не позднее даты начала срока действия *Сертификата* и *Технологического сертификата*.

4.3.УЦ обеспечивает доступ *Клиентов* и *Участников* к информации, содержащейся в реестре *Сертификатов* и *Технологических сертификатов* в сети Интернет на сайте www.authority.ru.

4.4.*УЦ* также может выполнять функции *Агента*, установленные Статьями 6, 7, 8, 9 настоящих Правил.

4.5.Срок действия *Сертификата Класса* 2, 3, 4 составляет один год с момента его создания *Удостоверяющим центром*. В отношении *Сертификатов Класса* 2, 3, 4 *УЦ* вправе, до истечения срока действия таких *Сертификатов*, изменить срок действия *Сертификата* с указанием причин такого изменения. Информация о причинах изменения срока действия *Сертификата*, новом сроке действия *Сертификата*, реквизитах такого *Сертификата* или информация, позволяющая иным образом идентифицировать такой *Сертификат/Сертификаты* публикуется в сети Интернет по адресу authority.ru, а также при наличии технической возможности направляется *Владельцу* соответствующего *Сертификата* в виде электронного документа. Изменение срока действия *Сертификата* происходит с момента подписания *Агентом* и *Владельцем Сертификата (Клиентом)* Акта приема-передачи, в котором указывается новый срок действия *Сертификата*. В случае не подписания по любым основаниям вышеуказанного Акта до истечения прежнего срока действия *Сертификата,* действие *Сертификата* прекращается, новый срок действия в отношении такого *Сертификата* не применяется. *Агент* вправе осуществлять подписание Актов приёма-передачи с указанием нового срока действия *Сертификата* только после получения от *УЦ* соответствующего уведомления в виде электронного документа с указанием *Сертификата*, в отношении которого подписание такого Акта возможно.

4.6.*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 неправомерным использованием. Все риски, связанные с использованием *Сертификатов*, *Технологических сертификатов*, *Криптографических ключей* несут *Клиент*ы, *Владельцы сертификатов*.

4.7.*УЦ* проверяет уникальность *Идентификатора владельца сертификата* в реестре *Сертификатов* и *Технологических сертификатов*.

4.8.*УЦ* осуществляет по обращениям *Участников* электронного взаимодействия проверку *ЭП*.

4.9.*УЦ* осуществляет иную связанную с использованием *ЭП* деятельность.

**Статья 5. Порядок создания и выдачи Технологических сертификатов**

5.1.Порядок создания и выдачи *Технологических сертификатов* определяется для каждого *Сервиса*

отдельным соглашением между *УЦ* и *Организатором каждого Сервиса*

**Статья 6. Общие положения о создании Сертификатов**

6.1.Создание *Сертификата* 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 собственноручной подписью *Клиента* или его *Уполномоченного лица*. Содержащиеся в Заявлении сведения подтверждаются предъявлением соответствующих документов (для физических лиц – паспорт; для представителей юридических лиц – паспорт, а также документ, подтверждающий право представителя действовать от имени данного юридического лица: доверенность, оформленная в соответствии с требованиями Гражданского кодекса Российской Федерации, учредительные документы юридического лица и иные документы, подтверждающие право действовать от имени юридического лица без доверенности). Проверку предоставленных *Клиентом* сведений производит *Агент*. По требованию *УЦ Агент* обязан направить в *УЦ* заверенную копию Заявления *Клиента* с отметкой *Агента* о его принятии, а также заверенные копии документов, предоставленных *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 ненаправления вышеуказанного Заявления и документов в установленный 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.Возможен иной порядок выдачи *Сертификатов* по согласованию с *УЦ*.

6.4.При возникновении технического сбоя передачи и/или обработки запроса на выдачу *Сертификата*, в результате которого *Агент / Клиент Агента* не получил запрошенный *Сертификат,* либо по иным причинам, фактически приведшим к неполучению *Агентом / Клиентом Агента* запрошенного *Сертификата, Агент* отправляет Заявление в форме *ЭД*, подписанного *ЭП Агента,* в *УЦ* с использованием программно-аппаратных средств *Агента*, подключенных через каналы связи к программно-техническим средствам *УЦ*. *Сертификат* признается сбойным, если заявление на объявление его сбойным поступает УЦ в определенном настоящим пунктом порядке в течение календарного месяца, в котором произошел технический сбой.

6.5.В случае если в течение календарного месяца, в котором возник технический сбой от *Агента* не поступит в УЦ запрос в виде ЭД 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.Создание *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 создании *Сертификатов* всегда проверяется уникальность *Идентификаторов владельцев сертификатов* (DN), принадлежащих разным *Владельцам сертификатов,* в реестре *Сертификатов* 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 настоящих Правил. Получив Заявление, подписанное *Клиентом*, идентифицировав Клиента и

проверив данные *Клиента* в соответствии с пунктом 6.1 настоящих Правил, *Агент* подтверждает запрос на создание *Сертификата*. Подтверждение запроса на выдачу *Сертификата Клиента* формируется Агентом 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, следующих за днём получения от *Агента* подтвержденного запроса в соответствии с п. 7.3 настоящих Правил.

7.5.*Агент* распечатывает на бумажном носителе Акт приема-передачи *Сертификата Клиента* по форме, установленной Приложением № 7 для *Клиента* - физического лица и Приложением № 8 для *Клиента* – юридического лица, в двух экземплярах и обеспечивает проставление в них собственноручной подписи *Клиента* или уполномоченного лица *Клиента*. Один подписанный Клиентом и Агентом экземпляр Акта приема-передачи на бумажном носителе хранится у *Агента*. По требованию *УЦ Агент* обязан направить *Удостоверяющему центру* заверенную копию Акта. Направление заверенной копии Акта осуществляется *Агентом* за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от *УЦ*. В случае ненаправления заверенной копии указанного выше Акта в установленный срок, *УЦ* вправе приостановить деятельность такого *Агента* по формированию запросов на создание *Сертификатов* и их выдаче *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, идентифицировав Клиента и проверив данные *Клиента* в соответствии с п. 6.1 настоящих Правил, *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, следующих за днём получения от *Агента* электронного запроса в соответствии с п. 8.1 настоящих Правил. Передача *УЦ* или уполномоченными им лицами *Агенту Ключевых носителей*, содержащих *Ключ ЭП* и *Сертификат*, созданные *УЦ* без получения Заявления от *Клиента*, осуществляется в порядке и на условиях, определяемых *УЦ* и *Агентом* дополнительно.

8.3.При создании *Сертификатов* всегда проверяется уникальность *Идентификаторов владельцев сертификатов* (DN), принадлежащих разным *Владельцам сертификатов*, и *Ключей проверки ЭП* в реестре Сертификатов и архиве *УЦ*. Программно-аппаратные средства *УЦ* исключают возможность создания одинаковых *Сертификатов*. При создании *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* по форме, установленной Приложением № 7 для *Клиента* - физического лица и Приложением № 8 для *Клиента* – юридического лица, в двух экземплярах и обеспечивает проставление в них собственноручной подписи *Клиента* или уполномоченного лица *Клиента*. Один подписанный Клиентом и Агентом экземпляр Акта приема-передачи на бумажном носителе хранится у *Агента*. По требованию *УЦ Агент* обязан направить *в УЦ* заверенную копию Акта. Направление заверенной копии Акта осуществляется *Агентом* за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от *УЦ*. В случае ненаправления Агентом заверенной копии указанного выше Акта в установленный настоящим пунктом срок, *УЦ* вправе приостановить деятельность такого *Агента* по формированию запросов на создание *Сертификатов* и их выдаче *Клиентам,* письменно уведомив об этом *Агента*.

**Статья 9. Порядок изготовления Сертификатов по 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,* при условии что *Клиент* идентифицирован *Агентом*.

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* вносится в реестр *Сертификатов*.

9.11. *Агент* вправе не хранить Акт в случае, когда Акт приема-передачи формируется в электронном виде и сохраняется *УЦ*.

9.12. *Агент* вправе 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 на сайте www.authority.ru.

10.2. Основанием для уплаты является счет, выставляемый *УЦ Агенту*. Уплата вознаграждения в соответствии с настоящим разделом осуществляется *Агентом* в течение 5 (Пяти) рабочих дней, следующих за днём 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 срока действия Сертификата определяется законодательством Российской Федерации.

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 Организатором *каждого Сервиса.*

**Статья 12. Права и обязанности Удостоверяющего центра**

12.1. *УЦ*, осуществляя создание *Сертификата Клиенту*, обеспечивает:

- внесение *Сертификата* в реестр *Сертификатов*;
- выдачу *Сертификата* обратившимся *Клиентам Сервиса*.

12.2. *УЦ* вправе отказать *Клиенту* в создании и выдаче *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 Агентом уплаты вознаграждения *УЦ*, предусмотренного Правилами, *УЦ* вправе взыскать с *Агента* неустойку в размере 0,1% от неуплаченной суммы за каждый день просрочки.

12.6. В случае прекращения деятельности *Агента (например,* в связи с отзывом лицензии, выданной Банком России на осуществление банковских операций в соответствии с Федеральным законом от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности») Соглашение о присоединении к Правилам считается расторгнутым со дня отзыва (аннулирования) лицензии *Агента* на осуществление банковских операций, *УЦ* вправе незамедлительно прекратить создание Сертификатов по заявлениям *Агента,* а также отключить доступ к программно-техническим средствам *УЦ*.

**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) и идентифицировать Клиента. *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 подписанные Клиентами Заявления *Клиента* и Акты приема-передачи в течение всего срока работы в качестве *Агента*. По запросу *УЦ*, а также при прекращении статуса *Агента, Агент* обязан в течение 15 (Пятнадцати) календарных дней передать Заявления *Клиентов* и Акты приема-передачи в *УЦ*. При несоблюдении обязательств, указанных в настоящем пункте, 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, путем направления УЦ соответствующего уведомления.

13.5. *Агент* обязан регулярно знакомиться с изменениями, вносимыми *Удостоверяющим центром* в настоящие Правила и публикуемыми *Удостоверяющим центром* в сети Интернет на сайте www.authority.ru.

**Статья 14. Права и обязанности Владельца сертификата**

14.1. *Владелец сертификата* обязан:

- использовать исключительно принадлежащие *Владельцу сертификата* уникальные *Ключи ЭП*;
- обеспечивать конфиденциальность *Ключи ЭП*;
- не использовать *Ключ ЭП* при наличии оснований полагать, что конфиденциальность данного *Ключа ЭП* нарушена;
- требовать приостановления действия *Сертификата* в корпоративной финансовой, информационной или иной системе, *Сервисе* при наличии подозрений на *Компрометацию ключа ЭП* в максимально сжатые сроки.

14.2. *Владелец сертификата* обязан регулярно знакомиться с изменениями, вносимыми *Удостоверяющим центром* в настоящие Правила, и публикуемыми *Удостоверяющим центром* в сети Интернет на сайте www.authority.ru.

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

15.1. *УЦ* имеет право в любое время в одностороннем порядке изменять настоящие Правила. *УЦ* размещает новую редакцию Правил в сети Интернет на сайте www.authority.ru не менее чем за 14 (Четырнадцать) календарных дней до вступления в силу новой редакции Правил.

15.2. Любые изменения в Правила. Вносимые Удостоверяющим центром, с момента вступления в силу новой Редакции Правил равно распространяются на всех лиц, присоединившихся к Правилам, в том числе присоединившихся к Правилам ранее даты вступления в силу новой редакции Правил.

15.3. *УЦ* имеет право в одностороннем порядке изменять Тарифы и условия уплаты вознаграждения. *УЦ* размещает новые тарифы в сети Интернет на сайте www.authority.ru не менее чем за 14 (Четырнадцать)

календарных дней до их вступления в силу. В случае, когда изменение Тарифов вызвано изменением стоимости оказания услуг партнерами *УЦ*, допускается сокращение срока размещения *Удостоверяющим центром* новых 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, если иное не указано в настоящих Правилах, и несут полную ответственность 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*, в соответствии с действующим законодательством Российской Федерации.

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*, создаваемые *УЦ*, в том числе персональные данные, не является 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, в том числе права 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* определены в Приложении № 2 к настоящим Правилам.

17.2. *Стороны* вправе расторгнуть отношения с *УЦ* в рамках настоящих Правил в одностороннем внесудебном порядке путем направления другой *Стороне* письменного уведомления не менее чем за 3 (Три) месяца 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, указанных в статье 10 настоящих Правил, более чем на 30 (Тридцать) календарных дней, *УЦ* вправе в одностороннем порядке приостановить исполнение своих обязательств, установленных 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.

17.6. *УЦ* несет ответственность за неисполнение или ненадлежащее исполнение своих обязательств, установленных настоящими Правилами, повлекшее причинение убытков *Агенту, Клиенту Агента*, третьим лицам, исключительно в размере документально подтвержденного и доказанного реального ущерба.

При этом размер возмещения реального ущерба, причиненного *Агенту,* в любом случае не может превышать размер вознаграждения *УЦ* за оказание определенной услуги в соответствии с настоящими Правилами, в отчетном месяце, в котором имело место неисполнение или ненадлежащее исполнение *УЦ* своих обязательств

при оказании такой услуги, за все нарушения, допущенные *УЦ* при оказании услуги в указанном отчетном месяце.

Указанное возмещение осуществляется только на основании письменного требования *Агента* с приложением соответствующих документов, доказывающих размер реального ущерба *Агента* и причинно-следственную связь указанного ущерба *Агента* с неисполнением или ненадлежащим исполнением обязательств *УЦ* при оказании услуги.

Упущенная выгода, которая может возникнуть у *Агента* вследствие неисполнения или ненадлежащего исполнения *УЦ* своих обязательств, возмещению не подлежит.

**Статья 18. Переходные положения**

18.1.Положения настоящих Правил имеют приоритет над условиями Договоров, заключенных между УЦ и *Агентами* после 01 апреля 2008 года.

**СОГЛАШЕНИЕ № _____**

**О ПРИСОЕДИНЕНИИ К ПРАВИЛАМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА «AUTHORITY»**

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 «AUTHORITY», которые размещены в сети Интернет 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 размещены в сети Интернет 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 «BeSafe» в качестве Агента Удостоверяющего центра на условиях Правил УЦ.

4. Удостоверяющий центр и Агент признают, что:

a. получение документа, подписанного Электронной подписью Агента, юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями уполномоченных лиц и оттиском печати (если она имеется) Агента. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки ЭП Агента созданы в соответствии с Правилами УЦ;

b. получение документа, подписанного Электронной подписью Удостоверяющего центра, юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями уполномоченных лиц Удостоверяющего центра и его оттиском печати (если она имеется). Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки Электронной подписи Удостоверяющего центра созданы в соответствии с Правилами УЦ.

5. Любая предварительная оплата по настоящему Соглашению не является коммерческим кредитом по смыслу ст. 823 Гражданского кодекса РФ. Стороны договорились о неприменении к правоотношениям Сторон положений ст. 317.1 Гражданского кодекса РФ в части начисления законных процентов.

6. Настоящее Соглашение вступает в силу с даты его подписания Сторонами, указанной в правом верхнем углу Соглашения.

7. Каждая из Сторон имеет право расторгнуть настоящее Соглашение в одностороннем порядке, предварительно направив уведомление другой Стороне не менее чем за 3 (Три) месяца до его расторжения.

8. Соглашение составлено в двух идентичных экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

**РЕКВИЗИТЫ СТОРОН**

| **УДОСТОВЕРЯЮЩИЙ ЦЕНТР:** | **АГЕНТ:** |
|---|---|
| Закрытое акционерное общество «Центр Цифровых Сертификатов» (ЗАО «ЦЦС»)<br>Адрес ЕГРЮЛ:<br>630055, г. Новосибирск, ул. Мусы Джалиля, д. 11, кабинет 309<br>Почтовый адрес:<br>630055, г. Новосибирск, ул. Шатурская, 2<br>Банковские реквизиты:<br>Р/с 40702810300000000075 в РНКО «Платежный Центр» (ООО)<br>БИК 045004832<br>К/с 30103810100000000832 в Сибирском ГУ Банка России<br>ИНН 5407187087<br>КПП 540801001 | |
| От Удостоверяющего центра | От Агента |
| _____ (_____) | _____ (_____) |
| М.п. | М.п. |

**Особенности создания Сертификатов для нужд Агентов** (распространяют свое действие на отношения УЦ и Агентов, возникшие с 01 мая 2015 года).

*1.* Для создания *Сертификата* для нужд *Агента, Агенту* необходимо подать в УЦ Заявление по форме, установленной Приложением № 6 к Правилам работы Удостоверяющего центра «AUTHORITY» (далее – «Правила УЦ») в письменной форме на бумажном носителе с приложением комплекта документов, подтверждающих указанные в Заявлении сведения.

*2.* УЦ в течение 3 (Трех) рабочих дней, следующих за днём получения Заявления и идентификации Агента, проверяет документы, создает и выдает *Сертификат Агенту* для обеспечения работы в качестве *Агента УЦ.*

*3.* После получения *Сертификата Агент* обязан направить в *УЦ* Заявление по форме, установленной Приложением №3 к настоящим Правилам (Заявление на регистрацию/отзыв прав доступа для *Сертификатов*). При передаче *УЦ Агенту Сертификата*, *УЦ* и *Агент* подписывают Акт приема-передачи по форме, определенной 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 на условиях настоящего Приложения к Правилам УЦ.*

*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, подписанное уполномоченным лицом Агента, направляется *Агентом* в *УЦ* в электронном (сканированном) виде на адрес электронной почты УЦ token@faktura.ru. Форма заявления определена в Приложении № 4 к Правилам.

*3.* Срок отправки *Смарт-ключей Агенту* составляет не более 2 (Двух) месяцев, следующих за днем оплаты *Агентом* счета.

*4.* Право собственности и риск случайной гибели *Смарт-ключей* переходят к *Агенту* с момента передачи *Смарт-ключей* первому перевозчику - транспортной организации (службы экспресс-доставки).

*5.* Обязательство *УЦ* по отправке *Смарт-ключей Агенту* считается выполненным с момента передачи их транспортной организации (службе 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 на сайте www.authority.ru.

**Приложение № 3**
к Правилам работы Удостоверяющего центра «AUTHORITY»
Заявление для УЦ от Агента на регистрацию прав сотрудников

Директору ЗАО «ЦЦС»
_____
от <Наименование Агента>

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

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

| № | ФИО Владельца сертификата | Значение *Идентификатора владельца сертификата Удостоверяющего центра* | Имя Сертификата | Права доступа | Предоставить/ отозвать | Адрес электронной почты |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |

Перечень прав доступа:

**Выдача Сертификатов** – право доступа, позволяющее сотруднику Агента осуществлять подтверждение запросов Клиентов на создание и выдачу Сертификатов в интерфейсе АРМ Администратора Ключей, а также подписывать акты приема-передачи Сертификатов Клиентам, при условии идентификации Клиента или уполномоченного лица Клиента, которому выдается Сертификат.

**Просмотр информации** – право доступа, позволяющее сотруднику Агента просматривать и выгружать информацию о Сертификатах в интерфейсе АРМ Администратора Ключей.

____ _____20___года

_____ (должность, реквизиты доверенности)

_____ /_____/
(Ф.И.О.)

М.П.

**Приложение № 4**
к Правилам работы Удостоверяющего центра «AUTHORITY»
Заявка на поставку Смарт-ключей

Директору ЗАО «ЦЦС»
От _____

**Заявка на поставку Смарт-ключей**

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

| Наименование Смарт-ключа | Количество, шт. |
|---|---|
| | |

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

| Подписано От Агента |
|---|
| _____ (_____) |
| 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» создать 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 размещены в сети Интернет на сайте www.besafe.ru ознакомлен(-а), соглас(-ен)(-на) и обязуюсь соблюдать и выполнять.

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

Реквизиты *Клиента*:

| | |
|---|---|
| ФИО | |
| Контактный телефон | |
| E-mail | |

Настоящим соглашаюсь с обработкой своих персональных данных Закрытым акционерным обществом «Центр Цифровых сертификатов», а также Агентом Удостоверяющего центра «AUTHORITY» и признаю, что персональные данные, включенные 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, реквизиты доверенности))

**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 размещены в сети Интернет на сайте www.besafe.ru ознакомлены, согласны и обязуемся соблюдать и выполнять.

Признаем, что получение документа, подписанного *Электронной подписью Участника Системы «BeSafe»* (далее – «*Участник*») юридически эквивалентно получению документа на бумажном носителе, подписанного 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 и используются в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY».

Реквизиты *Клиента*:

| | |
|---|---|
| ФИО уполномоченного лица организации | |
| Наименование организации | |
| Контактный телефон | |
| E-mail | |

Настоящим соглашаюсь с обработкой своих персональных данных Закрытым акционерным обществом «Центр Цифровых сертификатов», а также Агентом Удостоверяющего центра «AUTHORITY», и признаю, что персональные данные, включенные 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.**

**Приложение № 7**
к Правилам работы Удостоверяющего центра «AUTHORITY»
Акт приема-передачи Сертификата (физическое лицо)

**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 Агента >, 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 идентификацию Клиента, проверку данных *Клиента*, *Удостоверяющий центр* осуществил создание *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* и *Удостоверяющего центра* 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)

**Приложение № 8**
к Правилам работы Удостоверяющего центра «AUTHORITY»
Акт приема-передачи Сертификата (юридическое лицо)

**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 Агента >, 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 идентификацию Клиента, проверку данных *Клиента*, *Удостоверяющий центр* осуществил создание *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* и *Удостоверяющего центра* 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* | Назначение *Сертификата* указанного *Класса* |
|---|---|---|
| Класс 2 | CN = Class 2 CA<br>O = Center of Financial Technologies<br>C = RU | |
| Класс 3 | CN = Class 3 CA<br>O = Center of Financial Technologies<br>C = RU | |
| Класс 4 | CN = Class 4 CA<br>O = Center of Financial Technologies<br>C = RU | |

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

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