Утверждено
общим собранием участников
Общества с ограниченной ответственностью
«Компания Брокеркредитсервис»
Протокол № 12 от 12 апреля 2013 г.

Согласовано
Общество с ограниченной ответственностью
«Удостоверяющий центр БКС»
12 апреля 2013 г.

Соглашение
об использовании электронной подписи в корпоративной системе электронного документооборота «BCS»
(Приложение № 17)

г. Новосибирск

1. Общие положения

1.1 Настоящее Приложение № 17 к Регламенту оказания услуг на рынке ценных бумаг Общества с ограниченной ответственностью «Компания Брокеркредитсервис» (далее – Регламент) содержит существенные условия «Соглашения об использовании электронной подписи в корпоративной системе электронного документооборота «BCS» (далее – Соглашение), которое является дополнением к Генеральному Соглашению «О комплексном обслуживании на рынке ценных бумаг» (далее – Генеральное Соглашение).

1.2 Настоящее Соглашение устанавливает принципы осуществления информационного взаимодействия с использованием электронного документооборота между Участниками Сервиса, а также требования к оформлению и содержанию электронных документов, их реквизиты, особенности порядка их обработки, исполнения и хранения.

1.3 Условия, зафиксированные в настоящем Соглашении, считаются акцептованными Клиентом и являются неотъемлемой частью Генерального Соглашения, заключенного между ООО «Компания БКС» и Клиентом, если в тексте Заявления на комплексное обслуживание на рынке ценных бумаг или Заявления об изменении условий акцепта Регламента, направленного Клиентом в ООО «Компания БКС» в порядке, предусмотренном Регламентом, содержится указание на «использование электронной подписи в системе электронного документооборота» либо с Клиентом заключено дополнительное соглашение об использовании электронной подписи в системе электронного документооборота «BCS» к Генеральному Соглашению.

1.4 Корпоративная система электронного документооборота «BCS» (далее Система) – корпоративная информационная система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в соответствии с настоящим Соглашением и Федеральным законом от 25 марта 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон).

1.5 Сервисом является часть Системы, предназначенная для финансового и/или информационного электронного обслуживания Клиентов Общества с ограниченной ответственностью «Компания Брокеркредитсервис» (ООО «Компания БКС»). Сервис предназначен для использования в корпоративной информационной системе электронных подписей Участников.

1.6 Защита электронного документооборота осуществляется при помощи программного обеспечения, включающего в себя «Document Security Engine Client» и «Document Security Engine Agent», разработчиком которого является Закрытое акционерное общество «Центр Финансовых Технологий». ООО «Компания БКС» обладает ограниченным неисключительным правом на использование данного программного обеспечения.

2. Термины и определения

2.1 **Система (Система «BCS»)** – корпоративная информационная система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в соответствии с настоящим Соглашением и Федеральным законом.

2.2 **Организатор Сервиса** – ООО «Компания БКС», являющееся Владельцем Системы и осуществляющее управление Сертификатами ключей проверки электронной подписи Клиентов Сервиса в рамках Сервиса, а также отвечающее за назначение прав и полномочий доступа к данным и совершению операций Клиентов Сервиса и их уполномоченных лиц в рамках Сервиса.

2.3 **Участник Сервиса (Участник)** – ООО «Компания БКС» (Организатор Сервиса) и/или Клиент Сервиса.

2.4 **Клиент Сервиса (Клиент)**- лицо, заключившее с ООО «Компания БКС» настоящее Соглашение.

2.5 **Удостоверяющий центр** – Общество с ограниченной ответственностью «Удостоверяющий Центр БКС», заключившее с Организатором Сервиса соответствующий договор и осуществляющее создание Сертификатов ключей проверки электронной подписи Участников на основании заключенного с Участником соглашения об оказании услуг удостоверяющего центра ООО «Удостоверяющий Центр БКС». Удостоверяющий центр через Организатора Сервиса осуществляет проверку сведений о Клиентах, необходимую для создания Сертификатов ключа проверки электронной подписи Клиента.

2.6 **Администратор безопасности Удостоверяющего центра (Администратор безопасности)** – должностное лицо Удостоверяющего центра, которое отвечает за выдачу и регистрацию в реестре Сертификатов ключей проверки электронной подписи Организатора Сервиса и Клиентов Сервиса.

2.7 **Электронный документооборот** – обмен электронными документами в Сервисе в соответствии с Федеральным законом и настоящим Соглашением.

2.8 **Электронный документ** – документ, документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах, соответствующая установленному Организатором Сервиса формату.

2.9 **Оригинальный письменный документ (оригинал документа)** –документ на бумажном носителе, содержащий все необходимые реквизиты, подписанный уполномоченным лицом Клиента Сервиса - юридического лица, либо подписанный Клиентом Сервиса – физическим лицом (уполномоченным лицом Клиента Сервиса) в присутствии лица, уполномоченного ООО «Компания БКС», либо подпись Клиента Сервиса- физического лица (уполномоченного лица Клиента Сервиса) на котором заверена нотариально.

2.10 **Формат электронного документа** – структура содержательной части электронного сообщения, на основе которого сформирован электронный документ, соответствующая требованиям Организатора Сервиса.

2.11 **Отправитель электронного документа (Отправитель)** – Участник, который направляет электронный документ с использованием Сервиса.

2.12 **Получатель электронного документа (Получатель)** - Участник, которому электронный документ отправлен с использованием Сервиса.

2.13 **Криптографический ключ (ключ)** – общее название ключей электронной подписи и ключей проверки электронной подписи.

2.14 **Сертификат ключа проверки электронной подписи** - документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, которые включают в себя ключ проверки электронной подписи. Сертификат ключа проверки электронной подписи выдается Удостоверяющим центром Клиенту Сервиса для подтверждения подлинности электронной подписи и идентификации владельца Сертификата ключа проверки электронной подписи. Порядок выдачи Сертификата ключа проверки электронной подписи определяется настоящим Соглашением и соглашением об оказании услуг удостоверяющего центра ООО «Удостоверяющий Центр БКС».

2.15 **Идентификатор** – имя владельца Сертификата ключа проверки электронной подписи и номер Генерального соглашения Клиента, которые входят в состав всех сертификатов ключей подписи владельца сертификата. Идентификатор уникален в рамках выдавшего Сертификат ключа проверки электронной подписи Удостоверяющего центра и позволяет отличать и однозначно идентифицировать владельца Сертификата ключа проверки электронной подписи в рамках Системы.

2.16 **Владелец Сертификата ключа проверки электронной подписи** –лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки электронной подписи и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

2.17 **Создание Сертификата ключа проверки электронной подписи** – осуществляемая Удостоверяющим центром совместно с Организатором Сервиса и Клиентом процедура изготовления, выдачи и занесения в реестр Сертификата ключа проверки электронной подписи.

2.18 **Регистрация Сертификата ключа проверки электронной подписи** – осуществляемая Организатором Сервиса процедура внесения в реестр сертификатов ключей проверки электронных подписей, которая производится при условии предоставления владельцем Сертификата ключа проверки электронной подписи криптографических ключей, а при необходимости регистрации Сертификата ключа проверки электронной подписи юридического лица также доказательств, подтверждающих полномочия физического лица – представителя данного Участника.

2.19 **Компрометация криптографического ключа (компрометация ключа)** – констатация владельцем криптографического ключа обстоятельств, при которых возможно несанкционированное использование ключа электронной подписи неуполномоченными лицами.

2.20 **Рабочее время Организатора Сервиса** – с 9-00 до 21-00 по Новосибирскому времени в рабочие дни.

2.21 **Рабочие дни** – дни пятидневной (с понедельника по пятницу) рабочей недели, за исключением нерабочих праздничных дней и дней, объявленных выходными в связи официальным переносом выходных дней; а также выходные дни, официально объявленные рабочими в связи официальным переносом выходных дней.

2.22 **Время реагирования на уведомление о компрометации ключей** – 1 час рабочего времени с момента получения уполномоченным должностным лицом Организатора сервиса письменного или устного уведомления о компрометации ключа.

2.23 **Электронная подпись** - усиленная неквалифицированная электронная подпись в соответствии с Федеральным законом, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

2.24 Термины и определения, не приведенные в настоящем Соглашении, трактуются участниками в соответствии с Федеральным законом, а также действующим гражданским законодательством РФ.

3. Предмет соглашения.

3.1 Предметом настоящего Соглашения являются условия и порядок использования электронного документооборота, в том числе электронной подписи Участников.

3.2 Предметом настоящего Соглашения также являются условия и порядок предоставления Клиенту Сервиса ключей, необходимых для проведения идентификации Клиента Сервиса.

3.3 Положения настоящего Соглашения применяются, если иное не будет предусмотрено законодательными или иными нормативно-правовыми актами РФ.

3.4 Настоящее Соглашение не регулирует вопросы обмена электронными сообщениями, не являющимися электронными документами в соответствии с настоящим Соглашением.

3.5 Настоящее Соглашение определяет:

3.5.1. порядок выдачи Клиентам криптографических ключей;

3.5.2. порядок регистрации Сертификатов ключей проверки электронной подписи в Сервисе;

3.5.3. порядок информационного взаимодействия, порядок учета и хранения электронных документов, порядок формирования подтверждений о получении электронного документа и другие особенности документооборота, связанные с обслуживанием Участников, в том числе порядок проверки электронной подписи.

3.6 Заголовки разделов Соглашения даны исключительно для облегчения ссылок на них и не должны приниматься во внимание при толковании настоящего Соглашения.

4. Права и обязанности сторон.

4.1. ООО «Компания БКС» вправе:

4.1.1. приостановить исполнение обязательств по настоящему Соглашению или отказаться от исполнения в случае непредставления со стороны Клиента Сервиса исполнения обязательства либо наличия обстоятельств, очевидно свидетельствующих о том, что исполнение не будет произведено в установленный срок, при наличии таких обязательств;

4.1.2. устанавливать дополнительные требования для возможности участия новых Клиентов в Сервисе с предварительным уведомлением Клиентов Сервиса не менее, чем за 30 (тридцать) дней до момента вступления в силу дополнительных требований.

4.2. ООО «Компания БКС» обязано:

4.2.1. не разглашать третьим лицам, за исключением Удостоверяющего центра, и иных случаев, предусмотренных законодательством РФ, идентификационной и иной конфиденциальной информации Клиента Сервиса, ставшей известной ООО «Компания БКС» в ходе исполнения своих обязательств по настоящему Соглашению;

4.2.2. по письменному заявлению Клиента Сервиса предоставлять ему копии исходящих от ООО «Компания БКС» электронных документов на бумажных носителях с подписью уполномоченного лица и приложением печати ООО «Компания БКС» за плату, не превышающую стоимости затрат на изготовление указанных копий.

4.2.3. незамедлительно известить Клиентов Сервиса в случае возникновения обстоятельствах, предусмотренных п. 9.1 настоящего Соглашения путем размещения информации на www-странице Организатора Сервиса в информационно-телекоммуникационной сети Интернет, если это является возможным;

4.2.4. не совершать иные действия, противоречащие условиям настоящего Соглашения и наносящие ущерб Клиенту Сервиса.

4.3. Клиент Сервиса вправе:

4.3.1. использовать криптографические ключи в рамках Сервиса исключительно в соответствии с настоящим Соглашением, если иное не установлено договором, заключенным между Клиентом Сервиса и Организатором Сервиса;

4.4. Клиент Сервиса обязан:

4.4.1. предоставить достоверные сведения Организатору Сервиса при создании и регистрации криптографических ключей;

4.4.2. хранить собственные ключи электронной подписи в тайне и принять все необходимые меры для предотвращения их компрометации в процессе хранения и использования;

4.4.3. создать одну или несколько резервных копий криптографических ключей и хранить их в месте, недоступном для третьих лиц;

4.4.4. использовать криптографические ключи исключительно в собственной личной или предпринимательской деятельности;

4.4.5. не предоставлять криптографические ключи для использования любым третьим лицам;

4.4.6. не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4.4.7. оплачивать в случае необходимости стоимость доставки Сертификатов ключей проверки электронной подписи в соответствии с указанным Клиентом способом. Указанные в настоящем пункте денежные средства ООО «Компания БКС» вправе списывать с брокерского счета Клиента в безакцептном порядке на основании информации, полученной от Удостоверяющего центра, о выдаче Клиенту Сервиса Сертификата ключа проверки электронной подписи и не поступлении оплаты стоимости доставки Сертификатов ключей проверки электронной подписи. Согласие на безакцептное списание с брокерского счета Клиента стоимости доставки Сертификатов ключей проверки электронной подписи считается полученным с момента подачи заявления с указанием в качестве способа доставки Сертификата ключа проверки электронной подписи «курьерской почтой»;

4.4.8. предотвращать раскрытие, и/или воспроизведение, и/или распространение любой информации, связанной с работой Сервиса и являющейся конфиденциальной, а также любой иной информации, которая становится доступной вследствие работы в Сервисе;

4.4.9. за 30 (тридцать) дней до окончания срока действия Сертификата ключа проверки электронной подписи принять меры по получению нового Сертификата ключа проверки электронной подписи;

4.4.10. в случае компрометации ключа предпринять действия, предусмотренные п. 6.6 настоящего Соглашения;

4.4.11. в случае возникновения ситуации, предусмотренной п. 9.1 настоящего соглашения, незамедлительно, с учетом сложившейся ситуации, и способом, доступным в сложившихся обстоятельствах, известить Организатора Сервиса о возникших обстоятельствах;

4.4.12. владельцы криптографических ключей обязаны самостоятельно хранить выданные им ключи в электронном виде, в том числе и по истечение срока действия Сертификата ключа проверки электронной подписи.

4.5. Клиент допускается к осуществлению электронного документооборота в Сервисе после выполнения всей совокупности следующих действий и условий:

4.5.1. присоединения к настоящему Соглашению в порядке, предусмотренном п. 1.3 настоящего Соглашения;

4.5.2. заключения Клиентом с Удостоверяющим центром соглашения об оказании услуг удостоверяющего центра ООО «Удостоверяющий центр БКС».;

4.5.3. создания Клиентом криптографических ключей с использованием средств электронной подписи Организатора Сервиса;

4.5.4. создания Клиенту Сервиса Сертификата ключа проверки электронной подписи. Создание Сертификата ключа проверки электронной подписи осуществляется Администратором безопасности в соответствии с соглашением об оказании услуг удостоверяющего центра ООО «Удостоверяющий центр БКС». Настоящим Клиент уполномочивает Организатора Сервиса предоставлять Удостоверяющему центру информацию о Клиенте, необходимую для выполнения условий настоящего Соглашения, а также уполномочивает Организатора Сервиса передать в Удостоверяющий центр все сведения о Клиенте, необходимые для выдачи Сертификата ключа проверки электронной подписи;

4.5.5. получения Клиентом Сертификата ключа проверки электронной подписи на конфиденциальном разделе Клиента на www-странице Организатора Сервиса либо непосредственно в офисе Организатора Сервиса;

4.5.6. подписания Клиентом Сертификата ключа проверки электронной подписи на бумажном носителе (в двух экземплярах, если Клиент является юридическим лицом) и направления их Организатору Сервиса посредством факсимильной или электронной связи с последующим направлением Организатору Сервиса оригиналов данных документов;

4.5.7. регистрации Организатором Сервиса Сертификата ключа проверки электронной подписи в Сервисе на основании полученного от Клиента и подписанного им или его уполномоченным представителем (если Клиент –юридическое лицо) Сертификата ключа проверки электронной подписи на бумажном носителе (в двух экземплярах, если Клиент является юридическим лицом), либо на основании информации, полученной Организатором Сервиса от Удостоверяющего центра о регистрации Удостоверяющим центром Сертификата ключа проверки электронной подписи в реестре сертификатов Удостоверяющего центра, осуществленного Удостоверяющим центром на основании Сертификата ключа проверки электронной подписи, полученного от Клиента и подписанного им или его уполномоченным представителем (если Клиент –юридическое лицо) на бумажном носителе;

4.5.8. обеспечения совместимости средств криптографической защиты информации, используемых Клиентом Сервиса со средствами криптографической защиты информации, используемых в Сервисе;

4.5.9. Клиент Сервиса получает доступ к работе в Сервисе с использованием электронной подписи в системе электронного документооборота немедленно после регистрации Сертификата ключа проверки электронной подписи в Сервисе, осуществляемой Организатором Сервиса;

4.5.10. после регистрации Сертификата ключа проверки электронной подписи в Сервисе Организатор Сервиса направляет Клиенту один экземпляр Сертификата ключа проверки электронной подписи, содержащий подписи владельца Сертификата ключа проверки электронной подписи и Администратора

безопасности, в случае если Клиент в письменной форме заявлял о выдаче ему Сертификата ключа проверки электронной подписи на бумажном носителе и указанный Сертификата ключа проверки электронной подписи передан Удостоверяющим центром Организатору Сервиса. При этом Организатор Сервиса несет ответственность за сохранность Сертификата ключа проверки электронной подписи до момента передачи их организации связи.

5. Электронный документ

5.1. Электронный документ, сформированный в Сервисе, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в соответствии с настоящим Соглашением и действующим законодательством Российской Федерации, а также дополнительными договорами, заключенными между Участниками.

5.2. Электронный документ, используемый в Сервисе, считается надлежащим образом оформленным при условии его соответствия законодательству Российской Федерации, настоящему Соглашению, а также дополнительным договорам, заключаемым между Участниками, при наличии таковых.

Использование электронной подписи

5.3. Электронный документ должен быть подписан электронной подписью владельца криптографических ключей, Сертификат ключа проверки электронной подписи которого зарегистрирован за Клиентом Сервиса в порядке, установленном настоящим Соглашением.

5.4. Предусмотренные для электронного документа правовые последствия могут наступить, только если получен положительный результат проверки электронной подписи этого электронного документа. Проверка электронной подписи осуществляется программным обеспечением Системы (средствами электронной подписи Организатора Сервиса),

5.5. Электронный документ без электронной подписи, или имеющий формат, не отвечающий установленному соглашением сторон, в качестве электронного документа в рамках Системы в соответствии с настоящим Соглашением не рассматривается.

5.6. Электронный документ считается подписанным Участником, если он заверен электронной подписью, Сертификат ключа проверки электронной подписи которой зарегистрирован за ним. Риск неправомерного подписания электронного документа несет Участник, на имя которого зарегистрирован ключ электронной подписи.

5.7. Электронная подпись в электронном документе, Сертификат ключа проверки электронной подписи которой зарегистрирован за юридическим лицом (владельцем которого является юридическое лицо), признается равнозначной собственноручной подписи уполномоченного лица владельца Сертификата ключа проверки электронной подписи в документе на бумажном носителе, с приложением печати юридического лица-Участника Сервиса. При проверке документов для регистрации такого Сертификата ключа проверки электронной подписи за юридическим лицом, Организатор Сервиса проверяет документы самого юридического лица, а также полномочия уполномоченного лица на право осуществления действий от имени юридического лица в Сервисе.

Использование электронного документа

5.8. Весь документооборот (документы, поручения, распоряжения, отчеты, письма, уведомления, иное), оформляемый Участником в виде электронных документов в соответствии с настоящим Соглашением, а также договорами, заключенными между Участниками, признаётся совершенным в письменной форме и не может быть оспорен при одновременном выполнении следующих условий:

5.8.1. подтверждена подлинность электронной подписи в электронном документе с использованием соответствующих средств криптографической защиты информации, разрешённых к использованию Удостоверяющим центром;

5.8.2. Сертификат ключа проверки электронной подписи, относящийся к этой электронной подписи, не утратил силу (действует) на момент подписания и на момент получения электронного документа;

5.8.3. электронный документ учтён Организатором Сервиса, согласно правилам учета электронных документов в соответствии с п.п. 7.8 - 7.11 настоящего Соглашения;

5.8.4. электронная подпись используется в отношениях, регламентируемых настоящим Соглашением, а также дополнительными договорами, заключаемыми между Участниками Сервиса.

5.9. Электронный документ признается полученным Получателем в случае учета электронного документа в Сервисе.

Подлинник электронного документа

5.10. Электронный документ может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего электронного документа осуществляется воспроизводство содержания документа вместе с электронной подписью.

5.11. Все экземпляры электронного документа являются подлинниками данного электронного документа.

5.12. Электронный документ не может иметь копий в электронном виде.

5.13. Подлинник электронного документа считается не существующим в случаях, если:

5.13.1. не существует ни одного учтенного Организатором Сервиса экземпляра данного электронного документа и восстановление таковых невозможно;

5.13.2. не существует способа установить подлинность электронной подписи, которой подписан данный документ.

Копии электронного документа на бумажном носителе

5.14. Копии электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью уполномоченного лица Организатора Сервиса или Участника, являющегося Отправителем или Получателем.

5.15. Копии электронного документа на бумажном носителе должны соответствовать требованиям действующего законодательства РФ, а также содержать обязательную отметку «Копия электронного документа».

5.16. Информация, содержащаяся в копии на бумажном носителе, должна соответствовать содержанию электронного документа.

6. Криптографические ключи и Сертификаты ключей проверки электронной подписи

6.1. Одному идентификатору может соответствовать более чем один Сертификат ключа проверки электронной подписи.

Сертификаты ключей проверки электронной подписи

6.2. Содержание информации в Сертификатах ключей проверки электронной подписи определяется соглашением об оказании услуг удостоверяющего центра ООО «Удостоверяющий центр БКС»..

6.3. До начала работы Клиента в Сервисе Сертификат ключа проверки электронной подписи должен быть зарегистрирован Организатором Сервиса.

6.4. Сертификатом ключа проверки электронной подписи подтверждается, что при создании Сертификата ключа проверки электронной подписи произведена проверка на уникальность Идентификатора, а также проверка документов и прочей информации в соответствии с порядком, установленным для заключения и/или изменения условий Генерального Соглашения «О комплексном обслуживании на рынке ценных бумаг».

6.5. Информация, содержащаяся в Сертификате ключа проверки электронной подписи, не является конфиденциальной, на нее не распространяется режим коммерческой тайны. Настоящим Клиент выражает согласие на включение в состав информации в Сертификате ключа проверки электронной подписи имени (наименования) и номера Генерального соглашения Клиента.

Порядок действий при компрометации криптографических ключей

6.6. В случае компрометации криптографических ключей владелец указанных криптографических ключей обязан незамедлительно и не позднее одного рабочего дня со дня получения информации о нарушении конфиденциальности ключа электронной подписи уведомить уполномоченное должностное лицо Организатора Сервиса и Удостоверяющего центра о компрометации ключей по телефону с указанием номера Генерального Соглашения, номера брокерского счета Клиента и Уникального регистрационного номера Сертификата ключа проверки электронной подписи, присвоенного Удостоверяющим центром.

6.7. Уведомление, предусмотренное п.6.6 настоящего Соглашения, считается поданным в отношении всех криптографических ключей Участника, которым соответствует содержащийся в указанном уведомлении номер Генерального соглашения и Уникальный регистрационный номер Сертификата ключа проверки электронной подписи, присвоенный Удостоверяющим центром.

6.8. Организатор Сервиса на основании уведомления, предусмотренного п.6.6 настоящего Соглашения, приостанавливает права и полномочия доступа владельца Сертификатов криптографических ключей к данным и совершению операций с использованием криптографических ключей, в отношении которых было подано указанное уведомление, на период до 96 часов. Организатор Сервиса приостанавливает на период до 96 часов права и полномочия доступа владельца Сертификатов криптографических ключей к данным и совершению операций с использованием криптографических ключей, в отношении которых Организатором Сервиса получена информация от Удостоверяющего центра о получении последним уведомления, предусмотренного п.6.6 настоящего Соглашения, если ранее Организатором Сервиса не осуществлены указанные действия на основании аналогичного уведомления, предусмотренного п.6.6 настоящего Соглашения, полученного Организатором Сервиса, и/или письменного уведомления о компрометации.

6.9. Владелец криптографических ключей, в отношении которых было подано уведомление, предусмотренное п.6.6 настоящего Соглашения, обязан предоставить уполномоченному должностному лицу Организатора Сервиса письменное уведомление о компрометации в течение 96 часов с момента уведомления, предусмотренного п.6.6 настоящего Соглашения. Письменное уведомление о компрометации должно содержать Идентификатор владельца Сертификата ключа проверки электронной подписи скомпрометированного ключа и Уникальный регистрационный номер Сертификата ключа проверки электронной подписи, присвоенный Удостоверяющим центром.

6.10. Уведомление о компрометации, предусмотренное п.6.9 настоящего Соглашения, считается предоставленным уполномоченному должностному лицу Организатора Сервиса с момента фактического получения указанным лицом такого уведомления.

6.11. Организатор Сервиса возобновляет действие прав и полномочий доступа к данным и совершению операций владельца Сертификатов криптографических ключей, в отношении которых было подано уведомление, предусмотренное п.6.6 настоящего Соглашения, по истечение 96 часов с момента совершения Организатором Сервиса действий, предусмотренных п. 6.8 настоящего Соглашения, в случае неполучения в течение указанного срока уведомления, предусмотренного п. 6.9 настоящего Соглашения. В случае неполучения Организатором Сервиса от владельца Сертификата криптографических ключей письменного уведомления о компрометации, в том числе в случае не направления владельцем Сертификата криптографических ключей уведомления, предусмотренного п.6.6 настоящего Соглашения, Организатор Сервиса возобновляет действие прав и полномочий доступа к данным и совершению операций владельца Сертификата криптографических ключей, в отношении которых Организатором Сервиса получена информация от Удостоверяющего центра о получении последним уведомления, предусмотренного п.6.6 настоящего Соглашения, по истечение 96 часов с момента совершения Организатором Сервиса на основании указанной информации действий, предусмотренных п. 6.8 настоящего Соглашения, если в течение указанного срока Организатором Сервиса не получена информация от Удостоверяющего центра о получении последним уведомления, аналогичного по содержанию уведомлению, предусмотренному п. 6.9 настоящего Соглашения.

6.12. Электронный документ, подписанный криптографическим ключом подписи, в отношении которого было подано уведомление, предусмотренное п.6.6 настоящего Соглашения, отправленный после совершения Организатором Сервиса действий, предусмотренных п. 6.8 настоящего Соглашения, и до совершения Организатором Сервиса действий, предусмотренных п. 6.11 настоящего Соглашения, признается ненадлежащим и не порождает никаких последствий для Отправителя и Получателя.

6.13. Датой и временем компрометации в рамках данного Сервиса считаются дата и время получения уполномоченным должностным лицом Организатора Сервиса:

6.13.1.уведомления о компрометации, предусмотренного п.6.6 настоящего Соглашения, в случае своевременного и надлежащего исполнения Владельцем криптографических ключей обязанности, предусмотренной п. 6.9 настоящего Соглашения;

6.13.2.письменного уведомления о компрометации, если указанное уведомление было получено Организатором Сервиса по истечение 96 часов с момента совершения Организатором Сервиса действий, предусмотренных п. 6.8 настоящего Соглашения, либо если владелец криптографических ключей не уведомлял уполномоченное должностное лицо Организатора Сервиса в порядке, предусмотренном п. 6.6 настоящего Соглашения;

6.13.3. информации от Удостоверяющего центра о получении последним уведомления, аналогичного по содержанию уведомлению, предусмотренному п. 6.9 настоящего Соглашения, если указанная информация была получена Организатором Сервиса по истечение 96 часов с момента совершения Организатором Сервиса действий, предусмотренных п. 6.8 настоящего Соглашения; либо если Владелец криптографических ключей не исполнил обязанности, предусмотренной п. 6.9 настоящего Соглашения; либо если Владелец криптографических ключей не уведомлял уполномоченное должностное лицо Организатора Сервиса путем направления письменного уведомления о компрометации.

6.14 .Скомпрометированными считаются все ключи подписи Участника, которым соответствует содержащийся в уведомлении Идентификатор владельца Сертификата ключа проверки электронной подписи и Уникальный регистрационный номер Сертификата ключа проверки электронной подписи, присвоенный Удостоверяющим центром.

6.15. Организатор Сервиса аннулирует права и полномочия доступа владельца Сертификатов скомпрометированных криптографических ключей к данным и совершению операций с использованием скомпрометированных криптографических ключей и прекращает прием документов, подписанных с использованием скомпрометированных криптографических ключей после наступления даты и времени компрометации.

6.16. Электронный документ, подписанный скомпрометированным криптографическим ключом и отправленный после совершения Организатором Сервиса действий, предусмотренных п. 6.14 настоящего Соглашения, признается ненадлежащим и не порождает никаких последствий для Отправителя и Получателя.

7. Организация электронного документооборота

7.1. Электронный документооборот может включать:

7.1.1. формирование электронного документа;
7.1.2. отправку и получение электронного документа;
7.1.3. проверку электронного документа;
7.1.4. подтверждение получения электронного документа;
7.1.5. отзыв электронного документа;
7.1.6. учет электронных документов (регистрацию входящих и исходящих электронных документов);
7.1.7. хранение электронных документов (ведение архивов электронных документов;
7.1.8. создание дополнительных экземпляров электронного документа;
7.1.9. создание бумажных копий электронного документа.

Формирование электронного документа

7.2. Формирование электронного документа осуществляется в следующем порядке:

7.2.1. формирование электронного сообщения в формате, установленном для данного электронного документа;

7.2.2. подписание сформированного электронного сообщения электронной подписью.

7.3. Электронный документ считается исходящим от Отправителя, за исключением следующих случаев:

7.3.1. если Получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что электронный документ не исходит от Отправителя, или

7.3.2. если Получатель знал или должен был знать, в том числе в результате выполнения проверки электронной подписи, о том, что получен искаженный электронный документ.

7.4. Особенности отправки и получения электронных документов могут устанавливаться также дополнительными договорами, заключаемыми между Участниками.

Проверка подлинности доставленного электронного документа

7.5. Проверка подлинности электронного документа включает:

7.5.1. проверку электронного документа на соответствие установленному для него формату;

7.5.2. проверку подлинности электронной подписи электронного документа.

7.6. В случае положительного результата проверки электронного документа, данный электронный документ признается надлежащим. В противном случае данный электронный документ считается не полученным, о чем Получатель может послать уведомление Отправителю.

Учет электронных документов

7.7. Учет электронных документов осуществляется путем ведения электронных журналов учета. Технология ведения электронных журналов учета включает программно-технологические процедуры заполнения и администрирования электронных журналов и средства хранения этой информации. Программные средства ведения электронных журналов учета являются составной частью программного обеспечения, используемого для организации электронного документооборота.

7.8. Особенности учета электронных документов в Системе определяются настоящим Соглашением, а также могут определяться дополнительными договорами, заключаемыми между Участниками.

7.9. Организатор Сервиса обеспечивает защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах учета электронных документов. Срок хранения учетных данных не может быть менее 5 лет.

7.10. Все электронные документы, учтенные в Системе, должны храниться в течение сроков, предусмотренных настоящим Соглашением. Электронные документы должны храниться в электронных архивах.

Хранение электронных документов

7.11. Если дополнительными договорами, заключаемыми между Участниками, не предусмотрено иное, электронные документы должны храниться в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения электронных документов не может быть менее пяти лет.

7.12. Хранение электронных документов должно сопровождаться хранением соответствующих электронных журналов учета, Сертификатов ключей проверки электронной подписи и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки электронной подписи хранимых электронных документов.

7.13. Обязанности хранения электронных документов возлагаются на Организатора Сервиса.

7.14. Для выполнения текущих работ по ведению электронных архивов в подсистемах обработки данных Сервиса Организатор Сервиса назначает ответственных лиц.

7.15. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного или преднамеренного уничтожения и/или искажения.

8. Система обеспечения информационной безопасности

8.1. Информация, содержащая персональные данные, и конфиденциальная информация в Сервисе подлежит защите от разглашения.

8.2. Соблюдение требований информационной безопасности при организации электронного документооборота обеспечивает:

8.2.1. конфиденциальность информации (расшифровать информацию могут только уполномоченные лица);

8.2.2. целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);

8.2.3. аутентичность информации (отправителем информации является именно тот, от чьего имени она отправлена).

8.3. Требования по информационной безопасности при организации электронного документооборота реализуются посредством применения программно-технических средств и организационных мер.

8.4. К программно-техническим средствам относятся:

8.4.1. программные средства, специально разработанные для осуществления электронного документооборота;

8.4.2. система паролей и идентификаторов для ограничения доступа пользователей и операторов к техническим и программным средствам системы электронного документооборота;

8.4.3. средства формирования и проверки электронной подписи;

8.4.4. средства криптографической защиты информации;

8.4.5. программно-аппаратные средства защиты от несанкционированного доступа;

8.4.6. средства защиты от программных вирусов;

8.4.7. средства защиты от иных угроз информационной безопасности.

8.5. К организационным мерам относятся:

8.5.1. размещение технических средств в помещениях с контролируемым доступом;

8.5.2. административные ограничения доступа к программно-аппаратным средствам;

8.5.3. задание режима использования пользователями и операторами паролей и Идентификаторов;

8.5.4. допуск к осуществлению документооборота только специально обученных и уполномоченных на то лиц;

8.5.5. поддержание программно-технических средств в исправном состоянии;

8.5.6. резервирование программно-технических средств;

8.5.7. обучение технического персонала;

8.5.8. защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).

8.6. Порядок использования средств криптографической защиты информации, применяемых в Сервисе, определяются настоящим Соглашением, а также дополнительными договорами, заключаемыми между Участниками.

9. Чрезвычайные ситуации при осуществлении электронного документооборота

9.1. К числу обстоятельств, которые способны послужить причиной возникновения чрезвычайных ситуаций, в том числе технических сбоев, относятся любые события и/или обстоятельства, которые, по оценке Организатора Сервиса временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить осуществление электронного документооборота.

9.2. В случае наступления обстоятельств, указанных в п. 9.1 настоящего Соглашения:

9.2.1. Клиент Сервиса обязан незамедлительно с учетом сложившейся ситуации и способом, доступным в сложившихся обстоятельствах, известить Организатора Сервиса о возникших обстоятельствах, способных послужить причиной возникновения чрезвычайных ситуаций;

9.2.2. Организатор Сервиса обязан незамедлительно известить Клиентов Сервиса о возникших обстоятельствах путем размещения информации на www-странице Организатора Сервиса в информационно-телекоммуникационной сети Интернет, если это является возможным.

9.2.3. Впоследствии Участник обязан письменным сообщением Организатору Сервиса подтвердить уведомление о возникших обстоятельствах, способных послужить причиной возникновения чрезвычайных ситуаций.

9.2.4. Для квалификации ситуации в качестве чрезвычайной ситуации, в том числе технического сбоя, достаточно решения Организатора Сервиса.

9.2.5. Решение Организатора Сервиса о квалификации сложившихся обстоятельств в качестве чрезвычайной ситуации (квалифицирующее решение Организатора Сервиса) оформляется документом, составленным в письменной форме и подписанным надлежащим образом уполномоченным лицом Организатора Сервиса. По требованию заинтересованных Участников Сервиса такое решение может быть представлено в виде электронного документа или в виде копии документа на бумажном носителе.

9.3. В случае признания Организатором Сервиса факта наступления чрезвычайной ситуации, электронный документооборот в рамках Сервиса может быть прекращен по решению Организатора Сервиса.

9.4. Одновременно с признанием ситуации чрезвычайной Организатор Сервиса приступает к разработке мер по урегулированию сложившейся чрезвычайной ситуации в Сервисе.

9.5. Возобновление электронного документооборота осуществляется по решению уполномоченного органа Организатора Сервиса.

Меры по урегулированию чрезвычайных ситуаций

9.6. В качестве мер по урегулированию сложившейся чрезвычайной ситуации Организатор Сервиса вправе:

9.6.1. прекратить или ограничить обращение всех или части электронных документов в Сервисе;

9.6.2. совместно с Участниками Сервиса определить порядок действий по урегулированию чрезвычайной ситуации;

9.6.3. потребовать от Участников безвозмездного и незамедлительного с учетом сложившихся обстоятельств представления Организатору Сервиса копий на бумажных носителях всех или части электронных документов, сформированных и обращавшихся в Сервисе за определенный период времени;

9.6.4. потребовать от Участников за их счет незамедлительного с учетом сложившихся обстоятельств восстановления, в том числе в виде копий на бумажных носителях всех или части электронных документов в Сервисе;

9.6.5. предусмотреть иные меры, направленные на преодоление чрезвычайной ситуации.

9.7. При принятии решений по урегулированию чрезвычайных ситуаций Организатора Сервиса вправе:

9.7.1. устанавливать сроки и форму уведомления Участников Сервиса о своих решениях;

9.7.2. устанавливать сроки и порядок исполнения своих решений;

9.7.3. обуславливать порядок вступления в силу своих решений определенными обстоятельствами.

9.8. Решения Организатора Сервиса по урегулированию чрезвычайной ситуации в Сервисе являются обязательными для исполнения Участниками Сервиса.

9.9.О решениях Организатора Сервиса и мерах по урегулированию чрезвычайной ситуации Участники уведомляются не позднее момента начала принятия мер в соответствии с принятым решением.

10. Разрешение конфликтных ситуаций и споров

10.1. Разрешение конфликтных ситуаций и споров, возникших в связи с осуществлением электронного документооборота в Сервисе осуществляется в соответствии с Регламентом, настоящим Соглашением и действующим законодательством РФ.

10.2. В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

10.2.1. не подтверждение подлинности электронных документов средствами проверки электронной подписи Получателя;

10.2.2. оспаривание факта формирования электронного документа;

10.2.3. оспаривание факта идентификации владельца сертификата ключа проверки электронной подписи, подписавшего документ;

10.2.4. заявление Участника Сервиса об искажении электронного документа;

10.2.5. оспаривание факта отправления и/или доставки электронного документа;

10.2.6. оспаривание соответствия экземпляров электронного документа и/или подлинника и копии электронного документа на бумажном носителе;

10.2.7. иные случаи возникновения конфликтных ситуаций, связанных с функционированием Сервиса.

Уведомление о конфликтной ситуации

10.3. В случае возникновения конфликтной ситуации Клиент Сервиса, предполагающий возникновение конфликтной ситуации, должен незамедлительно, но не позднее чем в течение двух рабочих дней после обнаружения обстоятельств, являющихся причиной возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации Организатору Сервиса.

10.4. В случае, если возникновение конфликтной ситуации предполагается Организатором Сервиса, последний должен незамедлительно, но не позднее чем в течение двух рабочих дней после возникновения (обнаружения) обстоятельств, являющихся причиной возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации Клиенту Сервиса.

10.5. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации.

10.6. Уведомление о наличии конфликтной ситуации оформляется и отправляется в виде электронного документа, либо составляется в письменной форме и направляется с нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату. Независимо от того, составлено уведомление в письменной форме или в виде электронного документа, оно должно содержать реквизиты электронного документа, а также фамилию, имя, отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

10.7. Сторона, которой направлено уведомление, обязана не позднее чем в течение трех рабочих дней с момента получения уведомления проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить отправителю уведомления информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

10.8. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если отправитель уведомления удовлетворен информацией, полученной от Участника Сервиса, которому было направлено уведомление.

10.9. Отправитель уведомления считается удовлетворенным полученной от Участника Сервиса информацией, если от него в течение 10 (десяти) дней, следующих за днем направления ему информации о результатах проверки не поступило письменного заявления о рассмотрении конфликтной ситуации технической комиссией.

Техническая комиссия

10.10. В случае, если отправитель уведомления не удовлетворен информацией, полученной от Участника Сервиса, которому направлялось уведомление, для рассмотрения конфликтной ситуации, на основании соответствующего решения Организатора Сервиса, по заявлению любой из участвующих сторон формируется техническая комиссия.

10.11. Если Участники, являющиеся сторонами в конфликтной ситуации, не договорятся об ином, в состав технической комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон и, по заявлению любой из сторон, представитель Организатора Сервиса и Удостоверяющего центра. В состав технической комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон.

10.12. Право представлять в технической комиссии соответствующую Сторону должно подтверждаться доверенностью, выданной каждому представителю на срок работы технической комиссии.

10.13. По инициативе любого из Участников к работе технической комиссии для проведения технической экспертизы могут привлекаться независимые эксперты без права голоса, обладающими необходимыми знаниями в области защиты информации, работы компьютерных информационных систем. Участник, привлекающий независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

10.14. Работа технической комиссии осуществляется по месту нахождения Организатора сервиса.

10.15. Сформированная техническая комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки электронного документа, его подлинности, а также о подписании электронного документа конкретной электронной подписью, идентичности отправленного и полученного электронного документа.

10.16. Техническая комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению ее членов, для выяснения причин и последствий возникновения конфликтной ситуации.

10.17. Техническая комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

10.18. По итогам работы технической комиссии составляется Акт, в котором содержится краткое изложение выводов технической комиссии. Помимо изложения выводов о работе технической комиссии Акт должен также содержать следующие данные:

10.18.1. состав технической комиссии с указанием сведений о квалификации каждого из ее членов;

10.18.2. краткое изложение обстоятельств возникшей конфликтной ситуации;

10.18.3. дату и место составления Акта;

10.18.4. даты и время начала и окончания работы технической комиссии;

10.18.5. мероприятия, проводимые технической комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;

10.18.6. выводы, к которым пришла техническая комиссия в результате проведенных мероприятий;

10.18.7. подписи членов технической комиссии;

10.18.8. указание на наличие особого мнение члена (членов) технической комиссии, в случае наличия такового.

10.19. Акт составляется в таком количестве экземпляров, чтобы каждая из сторон в конфликтной ситуации, а также Организатор сервиса имели по одному подлинному экземпляру составленного акта. По требованию члена технической комиссии ему может быть выдана заверенная Организатором сервиса копия Акта.

10.20. К Акту может прилагаться особое мнение члена (членов) технической комиссии, не согласных с выводами технической комиссии, указанными в Акте. Особое мнение составляется в произвольной форме в таком же количестве подлинных экземпляров, что и Акт, и составляет приложение к Акту.

10.21. Акт по итогам работы технической комиссии направляется Организатором сервиса сторонам конфликтной ситуации с нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

10.22. В случае, если конфликтная ситуация не урегулирована в результате работы технической комиссии, либо в иной ситуации, если Участник Сервиса считает, что его права при осуществлении электронного документооборота в рамках Сервиса были нарушены, ситуация разрешается в общем порядке, предусмотренном соглашением сторон.

11. Заключительные положения

11.1. Прекращение действия настоящего Соглашения и Приложений к нему не влияет на юридическую силу и действительность электронных документов, которыми Участники обменивались до прекращения действия настоящего Соглашения и Приложений к нему.