**УТВЕРЖДАЮ:**
**Директор ЗАО «ЗОЛОТАЯ КОРОНА»**

**_____ Смоленская В.А.**

**Редакция № 1 от 26 октября 2016 года**

# ПРАВИЛА СЕРВИСА
# «Электронный документооборот в рамках проекта «Единое окно в торговых сетях»»

Настоящие Правила сервиса «Электронный документооборот в рамках проекта «Единое окно в торговых сетях»» (далее – «Правила», «Сервис») определяют правила электронного документооборота в рамках проекта «Единое окно в торговых сетях», порядок и условия его использования Участниками. Текст действующих Правил размещается в сети Интернет по адресу http://service.cft.ru/Pages/agreements.aspx

Присоединение Участника к условиям Правил осуществляется путём заключения с Организатором сервиса соглашения, согласно условиям которого Участник присоединяется к условиям настоящих Правил. Организатором настоящего Сервиса является ЗАО «ЗОЛОТАЯ КОРОНА».

Изготовление цифровых сертификатов для осуществления электронного документооборота в рамках настоящих Правил осуществляет Удостоверяющий центр «AUTHORITY» в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY», размещенными на сайте www.authority.ru (далее – «Правила Удостоверяющего центра»).

Настоящие Правила в части использования сертификатов ключа проверки электронной подписи действуют в рамках правил электронного документооборота корпоративной информационной системы «BeSafe» (далее – «Система BeSafe»), текст которых представлен в сети Интернет по адресу www.besafe.ru (далее – «Правила BeSafe»). Присоединение Участника к условиям настоящих Правил означает также присоединение Участника к Правилам BeSafe. Под Участником в настоящих Правилах понимается Клиент в терминах Правил BeSafe.

Организатор сервиса в рамках Правил BeSafe и Правил Удостоверяющего центра имеет статус Организатора сервиса и Агента Удостоверяющего Центра (далее – «Агент УЦ»), позволяющий организовывать выдачу Участникам цифровых сертификатов, созданных Удостоверяющим центром.

Термины, используемые в настоящих Правилах, определяются в соответствии с определениями, данными в Правилах Удостоверяющего центра.

## 1. Предмет регулирования настоящих Правил

Предметом регулирования настоящих Правил является:

1.1. Определение основных принципов организации и проведения электронного документооборота между Участниками и Организатором сервиса (далее – «Стороны») в рамках заключенных между ними договоров;

1.2. Установление прав, обязанностей и ответственности Сторон в результате указанной в п. 1.1 настоящих Правил деятельности.

1.3. В связи с тем, что в рамках данных Правил Стороны действуют во исполнение заключенных между ними договоров, для достижения взаимных интересов, никаких дополнительных финансовых обязательств в результате исполнения прав и обязанностей, установленных данными Правилами, между Сторонами не возникает (если иное не предусмотрено настоящими Правилами либо иным соглашением Сторон).

## 2. Общие принципы Электронного документооборота

2.1. Электронный документооборот осуществляется в соответствии с Правилами «BeSafe» с учетом особенностей, установленных настоящими Правилами, и/или в соответствии с соглашениями Сторон. Все Электронные документы (далее – «ЭД») в рамках настоящих Правил проходят проверку принадлежности Электронной подписи (далее – «ЭП») в ЭД уполномоченным лицам Сторон и отсутствия искажений в данном ЭД.

2.2. Стороны признают, что:

– внесение изменений в ЭД после его подписания ЭП дает отрицательный результат проверки ЭП;

– каждый Участник несет ответственность за сохранность Ключей ЭП/Закрытых ключей своих уполномоченных лиц и за действия своего персонала при работе в Системе;

– моментом формирования ЭП принимается момент получения ЭД, подписанного ЭП, принимающей Стороной, отраженный в Электронном журнале Системы Организатора сервиса;

– Электронные документы юридически эквивалентны документам на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц с проставлением оттиска печати.

2.3. Для создания Ключей ЭП и Ключей проверки ЭП, подписания ЭД, проверки ЭП, зашифровывания и расшифровывания Электронных сообщений Стороны используют только совместимые Средства криптографической защиты информации (далее – «СКЗИ») и признают их достаточными для Подтверждения подлинности Электронной подписи в Электронном документе, для защиты от несанкционированного доступа, а также для обеспечения конфиденциальности, авторства и подлинности информации, содержащейся в пересылаемых ЭД. Список совместимых (разрешенных к использованию) СКЗИ представлен в Приложении № 2 к Правилам BeSafe.

2.4. Стороны принимают на себя все риски, связанные с работоспособностью своего оборудования, каналов связи, программного обеспечения, установленного на своих программно-аппаратных комплексах.

2.5. Стороны строго выполняют требования технической и эксплуатационной документации по системам защиты информации, обеспечивающие конфиденциальность, целостность и сохранность программных средств, ЭД, протоколов регистрации событий, действующей парольной и ключевой информации, используемой для доступа в Систему, кодирования данных и определения их авторства.

2.6. Стороны организовывают внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность использования Ключей ЭП не уполномоченными на то лицами.

2.7. Стороны принимают необходимые меры для исключения обмена ЭД, содержащими компьютерные вирусы и/или иные вредоносные программы.

2.8. Стороны обязуются своевременно информировать друг друга обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭД. В случае обнаружения возможных угроз безопасности ЭД Стороны обязуются своевременно извещать друг друга о них для принятия согласованных мер по защите.

2.9. Участники признают в качестве единой шкалы времени время часового пояса г. Новосибирска. Участники обязуются поддерживать системное время аппаратных средств, обеспечивающих работоспособность Системы, в соответствии с текущим астрономическим временем с точностью до пяти минут. При возникновении разногласий эталонным считается время, установленное на аппаратных средствах Организатора сервиса.

## 3. Особенности Электронного документооборота в рамках Соглашения

3.1. Порядок выдачи и регистрации Сертификата ключа проверки электронной подписи.

3.1.1. Уполномоченное лицо Участника самостоятельно изготавливает ключ электронной подписи, ключ проверки электронной подписи, сохраняя их в памяти своего персонального компьютера или на Смарт-ключах, и направляет Агенту УЦ заявление о создании Сертификата ключа проверки электронной подписи. Для этого уполномоченное лицо Участника, при необходимости, устанавливает требуемое программное обеспечение, заходит по ссылке https://www.authority.ru/auth/1st_class.jsp?class=3&type=2&f=fin&agentId=3802, заполняет отображаемую форму Заявления на выдачу Сертификата ключа проверки электронной подписи и отправляет заявление. Заявление формируется в виде Электронного документа и направляется Агенту УЦ с использованием программно-аппаратных средств Участника, подключенных через каналы связи к программно-техническим средствам Агента УЦ. После отправки заявления в электронном виде Участник направляет его Агенту УЦ в бумажном виде с собственноручной подписью уполномоченного лица Участника, действующего на основании учредительных документов (с заверением печатью Участника, если имеется) или доверенности (далее по тексту – «уполномоченное лицо Участника»), с приложением документов, подтверждающих личность и полномочия уполномоченного лица Участника (в доверенности должны быть обязательно указаны ФИО и должность/паспортные данные уполномоченного лица; при указании должности одновременно с доверенностью должна быть представлена заверенная копия документа о назначении на должность с указанием паспортных данных).

3.1.2. В течение 3 (Трёх) рабочих дней с момента получения Агентом УЦ заявления в бумажном виде, УЦ направляет Участнику изготовленный им Сертификат в электронном виде, либо мотивированный отказ от его выдачи. Участник направляет Агенту УЦ Акт приёма-передачи Сертификата ключа проверки электронной подписи в бумажном виде за подписью уполномоченного лица Участника.

3.1.3. Срок действия Сертификата – 1 (Один) год.

3.1.4. После получения Сертификата Участник передает Организатору полученный Сертификат, который содержит в себе Ключ проверки электронной подписи.

3.1.5. Участник направляет Организатору в бумажном виде заявку о регистрации Сертификата ключа проверки электронной подписи в роли «Администратор ключей точки обслуживания). Заявка должна быть заполнена в строгом соответствии с утвержденными формами (Приложение № 1 к настоящим Правилам) и подписана уполномоченным лицом Участника. Данный Сертификат используется для выдачи и регистрации Сертификатов точки обслуживания согласно п. 5.5. настоящих Правил, а также для подписания заявок на регистрацию пунктов Участника.

3.1.6. Сертификат может быть зарегистрирован только при условии получения Организатором всего пакета оригиналов документов на бумажном носителе и в надлежащей форме, а именно: Заявления на выдачу Сертификата, Акта приема-передачи Сертификата, Заявки на регистрацию Сертификата, доверенности, подтверждающей полномочия уполномоченных лиц Участника (при необходимости).

3.1.7. До истечения срока действия Сертификата уполномоченное лицо Участника должно изготовить и получить новые: Ключ электронной подписи, Ключ проверки электронной подписи и Сертификат ключа проверки электронной подписи в порядке, установленном п. 3.1.1. настоящих Правил, за исключением следующего: уполномоченное лицо Участника заходит по ссылке https://secure.authority.ru/auth/renew.jsp?agentId=3802 и не направляет Агенту УЦ Заявление на выдачу Сертификата ключа проверки электронной подписи, Акта приёма-передачи Сертификата ключа проверки электронной подписи и Заявки на регистрацию Сертификата ключа проверки электронной подписи в бумажном виде, вместо этого, Участник подтверждает свое заявление, акт приёма-передачи и заявку в электронном виде действующим Сертификатом ключа проверки электронной подписи.

3.1.8. Участник несет полную ответственность по всем операциям, подтвержденным любым Сертификатом Участника.

3.1.9. Организатор получает и регистрирует Сертификаты на свое имя в том же порядке, что предусмотрен настоящими Правилами для Участника.

3.1.10. Участник обязуется обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование кем-либо принадлежащих Участнику Ключей электронных подписей без его согласия. При компрометации/аннулировании (отзыве) Ключа электронной подписи Участник обязан незамедлительно сформировать и направить Организатору уведомление о компрометации/аннулировании Ключа электронной подписи в соответствии с утвержденной в Приложении № 2 к настоящим Правилам формой в электронном виде на адрес https://jira.korona.net с последующей отправкой в бумажном виде. В течение 24 (Двадцати четырёх) часов с даты получения уведомления в электронном виде Организатор блокирует Сертификат, однозначно связанный со скомпрометированным Ключом электронной подписи для работы в рамках Правил. До момента блокировки Сертификата Электронные документы, направленные с использованием скомпрометированного Ключа электронной подписи, считаются направленными Участником и последний несет всю полноту ответственности за совершенные с использованием такого Сертификата действия.

3.1.11. При изменении уполномоченного лица Участника или его данных, отзыва доверенности, Участник обязуется направить Организатору сервиса уведомление об аннулировании Ключа электронной подписи в порядке, предусмотренном п. 3.1.10 настоящих Правил.

3.1.12. Удостоверяющий центр, Организатор, Агент УЦ не несут ответственности за несанкционированное использование Сертификатов, а также за ущерб, причиненный Участнику или уполномоченному лицу Участника таким использованием.

3.1.13. Электронные документы признаются полученными с момента получения Электронного документа получателем Электронного документа.

3.1.14. Действуют Сертификаты ключей электронной подписи Класса 3.

3.1.15. Стороны не вправе осуществлять отзыв отправленных Электронных документов.

**5. Дополнительные положения, действующие самостоятельно, вне Правил Besafe**

5.1. Для получения Сертификата точки обслуживания (Технологического сертификата 5 класса) Участник оформляет заявление по ссылке

https://www.authority.ru/auth/1st_class.jsp?class=5&type=2&f=fin&agentId=3802. Сертификат точки обслуживания является технологическим сертификатом, создаваемым в соответствии с Правилами Удостоверяющего центра. Заявление формируется в виде электронного документа и направляется Агенту УЦ. После отправки заявления в электронном виде Участник направляет его Агенту УЦ в бумажном виде с собственноручной подписью уполномоченного лица Участника, с приложением документов, подтверждающих личность и полномочия уполномоченного лица.

5.2. В течение 3 (Трёх) рабочих дней с момента получения Агентом УЦ заявления в бумажном виде, УЦ направляет Участнику изготовленный им Сертификат точки обслуживания в электронном виде, либо мотивированный отказ от его выдачи. Участник направляет Агенту УЦ акт приёма-передачи Сертификата точки обслуживания в бумажном виде за подписью уполномоченного лица Участника.

5.3. Участник регистрирует указанный Сертификат точки обслуживания в Системе, направив заявку в бумажном виде (форма представлена в Приложении № 3 к настоящим Правилам) Организатору. Сертификат точки обслуживания регистрируется с целью идентификации Пункта Участника в Системе.

5.4. Срок хранения Сертификата точки обслуживания в Удостоверяющем Центре неограничен, однако в целях обеспечения защиты информации в связи с применяемой технологией срок использования Сертификатов точки обслуживания ограничен 3 (Тремя) годами. По истечении указанного срока Сертификат точки обслуживания блокируется.

5.5. Выдача и регистрация Сертификатов точки обслуживания может также происходить путем формирования представителем Участника, зарегистрированным в роли «Администратор ключей точки обслуживания», соответствующих заявлений. Администратор ключей точки обслуживания, используя АРМ «Администратор», создает и подписывает заявление на получение сертификата точки обслуживания своей Электронной подписью. После получения Сертификата точки обслуживания Администратор ключей точки обслуживания формирует заявление на регистрацию сертификата точки обслуживания.

5.6. Стороны признают, что все действия, совершенные с использованием Сертификата точки обслуживания, признаются действиями, совершенными Участником в лице уполномоченного им и указанного в сертификате лица.

**Приложение № 1**
**к Правилам сервиса «Электронный документооборот**
**в рамках проекта «Единое окно в торговых сетях»»**

*ОБРАЗЕЦ*
Печатается на бланке Участника

**Директору**
**ЗАО «ЗОЛОТАЯ КОРОНА»**
**Смоленской В.А.**

**ЗАЯВКА НА РЕГИСТРАЦИЮ**
**СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ**

_____ (далее – «Участник») в лице ____, действующего на основании ___, настоящим просит зарегистрировать Сертификат ключа проверки электронной подписи (далее – «Сертификат») с целью осуществления действий в соответствии с Соглашением об услугах № _____ от _ _____ 201_ года:

| | |
|---|---|
| Наименование Участника | |
| ФИО уполномоченного лица Участника | |
| Идентификатор Владельца сертификата | |
| Серийный номер Сертификата | |
| Контакты Владельца сертификата (тел., факс, e-mail) | |
| Эмитент Сертификата (поле – «Издатель») | |
| IP-адрес(а)/адрес электронной почты, с которого (ых) будет направляться информация в электронной форме, подписанная электронной подписью | |
| Роль Участника | Администратор ключей точки обслуживания |

Подтверждаем, что Ключ электронной подписи, Ключ проверки электронной подписи и Сертификат ключа проверки электронной подписи созданы в соответствии с правилами КИС «BeSafe».

Подтверждаем полное и безусловное согласие со всеми условиями Правил КИС «BeSafe».

Информация в электронной форме, подписанная электронной подписью, которой соответствует указанный в настоящей заявке Сертификат ключа проверки электронной подписи, и переданная в рамках Соглашения об услугах № _____ от _ _____ 201_ года, является равнозначной документу на бумажном носителе, подписанному собственноручной подписью лица, действующего от имени Участника на основании учредительных документов или доверенности.

С момента направления указанной заявки Участник в полном объеме несет ответственность по всем операциям, подтвержденным указанным Сертификатом.

**Участник:**

✍

*Подпись* *Фамилия И.О.*

**Дата: "_____" _____ 201__**

**Приложение № 2**
**к Правилам сервиса «Электронный документооборот**
**в рамках проекта «Единое окно в торговых сетях»»**

*ОБРАЗЕЦ*
Печатается на бланке Участника

**Директору**
**ЗАО «ЗОЛОТАЯ КОРОНА»**
**Смоленской В.А.**

**УВЕДОМЛЕНИЕ О КОМПРОМЕНТАЦИИ/АННУЛИРОВАНИИ**

_____ (далее – «Участник») в лице ____, действующего на основании ___, настоящим сообщает о факте компрометации/аннулирования Ключа электронной подписи, которому соответствует указанный ниже Сертификат ключа проверки электронной подписи:

| | |
|---|---|
| Наименование Участника | |
| ФИО Владельца сертификата (физическое лицо, действующее от имени Участника) | |
| Идентификатор Владельца сертификата | |
| Контакты Владельца сертификата (тел., факс, e-mail) | |

Прошу блокировать указанный Ключ электронной подписи для работы в рамках Соглашения об услугах № _____ от _ _____ 201_ года.

**Участник:**

✍

*Подпись* *Фамилия И.О.*

**Дата: "_____" _____ 201__г.**

**Приложение № 3**
**к Правилам сервиса «Электронный документооборот**
**в рамках проекта «Единое окно в торговых сетях»»**

*ОБРАЗЕЦ*
Печатается на бланке Участника

**Директору**
**ЗАО «ЗОЛОТАЯ КОРОНА»**
**Смоленской В.А.**

**ЗАЯВКА НА РЕГИСТРАЦИЮ СЕРТИФИКАТОВ ТОЧЕК ОБСЛУЖИВАНИЯ УЧАСТНИКА**

_____ (далее – «Участник»), в лице _____, действующего на основании _____, настоящим просит зарегистрировать сертификаты точек обслуживания Участника со следующими параметрами:

| № п/п | Адрес точки обслуживания Участника | Контакты точки обслуживания (тел., факс, e-mail) | Эмитент сертификата (поле – «Издатель») | Владелец сертификата (поле – «Субъект») | Отпечаток сертификата по алгоритму sha1 | Открытый ключ сертификата | Алгоритм ключа сертификата |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Признаем, что все действия, совершенные в Сервисе «Единое окно в торговых сетях» с использованием соответствующего данному сертификату ключа, совершены Участником.

**Участник:**

_____ ✍ _____ _____

*Должность (либо доверенность)* *Подпись* *Фамилия И.О.*

*М.П.*

**Дата: "_____" _____ 201__**

**Приложение № 4**
**к Правилам сервиса «Электронный документооборот**
**в рамках проекта «Единое окно в торговых сетях»»**

ДОВЕРЕННОСТЬ
(предлагаемая форма)

г. _____ ___ _____ _____ года

_____ (Организационно-правовая форма и наименование организации, ИНН, ОГРН) в лице _____ (должность и ФИО уполномоченного лица организации), действующего на основании Устава, далее – «Участник», настоящей доверенностью уполномочивает _____ (ФИО, дата рождения, паспортные данные поверенного) на совершение от имени Участника действий, предусмотренных Правилами сервиса «Электронный документооборот в рамках проекта «Единое окно в торговых сетях»» и Правилами электронного документооборота корпоративной информационной системы «BeSafe», размещенных в сети интернет по адресам соответственно: http://service.cft.ru/Pages/agreements.aspx и www.besafe.ru, включая подписание любых необходимых документов, предусмотренных указанными правилами, в том числе:

1. Заявлений на выдачу Сертификатов ключей проверки электронной подписи;
2. Заявок на регистрацию Сертификатов ключей проверки электронной подписи;
3. Актов приема-передачи Сертификатов ключей проверки электронной подписи;
4. Уведомлений о компрометации/аннулировании (отзыве) Ключей электронной подписи;
5. Заявлений на выдачу, заявок на регистрацию Сертификатов Точек обслуживания Участника,

а также совершения от имени Участника любых действий с использованием полученного Сертификата ключа проверки электронной подписи, Сертификатов Точек обслуживания.

Подпись уполномоченного лица _____ удостоверяю.

Доверенность выдана сроком до ___ _____ _____ года без права передоверия третьим лицам.

| _____ | _____ | _____ |
|---|---|---|
| (должность, наименование организации) | | (ФИО) |