Приложение № 2

к Приказу ООО КБ «Металлург»

 № 310 от «30» декабря 2016г.

Порядок получения ключей электронной подписи клиентами

ООО КБ «Металлург»

1. Положение о работе Удостоверяющего Центра

 1.1. Настоящий Порядок определяет порядок и условия изготовления, распространения Сертификатов ключей проверки электронной подписи и Сертификатов ключей шифрования и прекращения срока их действия.

2. Термины и определения

Система - Корпоративная информационная система «BeSafe» - совокупность программного, информационного и аппаратного обеспечения, позволяющая организовать электронный документооборот. Правила Системы размещены в Интернете на веб-сервере по адресу  **www.besafe.ru.**

Удостоверяющий центр (УЦ) – удостоверяющий центр (удостоверяющий центр «Authority»), созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов», который осуществляет изготовление Сертификатов для юридических и физических лиц в целях возможности осуществления электронного документооборота в рамках КИС «BeSafe». Удостоверяющий центр или уполномоченные им представители (Агенты) осуществляют проверку Клиентов и документов Клиентов, необходимых для создания Сертификатов Клиента.

Банк – Общество с ограниченной ответственностью Коммерческий банк «Металлург».

Агент (Доверенное лицо) - уполномоченный представитель Удостоверяющего центра, которым является Общество с ограниченной ответственностью Коммерческий Банк «Металлург», заключивший с Удостоверяющим центром договор, в соответствии с которым Банк осуществляет проверку Клиентов, документов Клиентов, предшествующую изготовлению Удостоверяющим центром Сертификатов, направляющий или подтверждающий Удостоверяющему центру запрос на изготовление Сертификата и организующий передачу Клиенту Ключевого носителя, содержащего Сертификат, изготовленный Удостоверяющим центром. Агент в случае необходимости осуществляет выдачу Клиентам Ключевых носителей, содержащих Криптографические ключи, Сертификаты, изготовленные Удостоверяющим центром, в порядке, предусмотренном настоящими Правилами.

 Клиент - физическое лицо, предприниматель без образования юридического лица, юридическое лицо, имеющие в Банке открытый счет.

Участник – УЦ, Агент или Клиент в соответствии с настоящим Порядком.

Правила - Правила работы Удостоверяющего центра «AUTHORITY».

Шифрование - криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

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

Класс сертификата - атрибут Сертификата, характеризующий процедуру проверки, которую прошёл Владелец сертификата при создании Сертификата.

Идентификатор владельца сертификата - идентификационные данные Владельца сертификата, которые входят в состав Сертификата. Идентификатор владельца сертификата позволяет отличать и однозначно идентифицировать Владельца сертификата в рамках Системы. Идентификаторы владельцев сертификатов одного Класса, принадлежащие разным Владельцам сертификатов, уникальны в рамках выдавшего Сертификаты УЦ. Уникальность Идентификаторов владельцев сертификатов одного Класса, принадлежащих разным Владельцам сертификатов, обеспечена технологическими средствами УЦ при условии, что Владелец сертификата не допустил Компрометации собственных Ключей ЭП.

Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме и заверена Электронной подписью. Электронный документ может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

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

Закрытый (секретный) ключ - Ключ ЭП или Закрытый (секретный) ключ шифрования.

Открытый ключ - Ключ проверки ЭП или Открытый ключ шифрования. Криптографические ключи - общее название Открытых и Закрытых ключей.

Сертификат - общее название Сертификатов ключей проверки ЭП и Сертификатов ключей шифрования, использование которых регулируется правилами Системы и настоящим Порядком.

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

Средства электронной подписи (Средства ЭП) - аппаратные и/или программные средства, являющиеся частью средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации электронного документооборота: создание ЭП в ЭД с использованием Ключа ЭП; подтверждение подлинности ЭП, содержащейся в ЭД, с использованием Ключа проверки ЭП; создание Ключей ЭП и Ключей проверки ЭП.

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

Владелец сертификата ключа проверки ЭП (Владелец сертификата ключа подписи) - физическое или юридическое лицо, на имя которого УЦ выдан Сертификат и которое владеет соответствующим Ключом ЭП, позволяющим с помощью средств ЭП создавать ЭП в ЭД (подписывать ЭД).

Ключ ЭП (Закрытый (секретный) ключ электронной цифровой подписи) - последовательность символов, известная Владельцу сертификата и предназначенная для создания в ЭД Электронной подписи с использованием средств ЭП.

Ключ проверки ЭП (Открытый ключ ЭП) - последовательность символов, соответствующая Ключу ЭП, предназначенная для подтверждения (проверки) с использованием средств ЭП подлинности ЭП в Электронном документе.

Сертификат ключа проверки ЭП (Сертификат ключа подписи) - ЭД с Электронной подписью УЦ, доступный любому Участнику, включающий в себя Ключ проверки ЭП Владельца сертификата. Сертификаты выдаются УЦ Участнику для подтверждения подлинности ЭП и идентификации Владельца сертификата. Сертификат уникален в рамках выдавшего его УЦ.

Владелец ключа шифрования (Владелец сертификата ключа шифрования) - физическое или юридическое лицо, на имя которого УЦ изготовлен Сертификат и которое обладает соответствующим Закрытым ключом шифрования.

Владелец сертификата - общее название Владельцев сертификатов ключей проверки ЭП и Владельцев ключей шифрования.

Закрытый (секретный) ключ шифрования - последовательность символов, известная Владельцу ключа шифрования и предназначенная для расшифровывания ЭД.

Открытый ключ шифрования - последовательность символов, предназначенная для зашифровывания ЭД, предназначенных Владельцу ключа шифрования.

Сертификат ключа шифрования - документ на бумажном носителе или Электронный документ с Электронной подписью УЦ, доступный любому Участнику, включающий Открытый ключ шифрования Владельца ключа шифрования. Сертификат ключа шифрования создаётся УЦ для обеспечения возможности шифрования предназначенных Владельцу сертификата ключа шифрования ЭД. Сертификат ключа шифрования уникален в рамках выдавшего его УЦ.

Создание сертификата - осуществляемая УЦ процедура изготовления, выдачи и занесения в реестр Сертификата или Технологического сертификата.

Технологический сертификат – общее название сертификатов, не используемых для юридически значимого документооборота в рамках Системы, не предназначены для использования в качестве Сертификатов в рамках правил Системы.

Компрометация ключа - нарушение конфиденциальности Закрытого ключа, констатация Владельцем сертификата обстоятельств или наступление обстоятельств, при которых возможно несанкционированное использование Закрытого ключа неуполномоченными лицами.

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

3. Правовое регулирование отношений в области использования Сертификатов

1. Правовое регулирование отношений в области изготовления и распространения Сертификатов УЦ осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (в части касающейся деятельности Системы), Гражданским Кодексом РФ, Правилами, настоящим Порядком, а также договорами и соглашениями участников электронного документооборота.
2. Настоящий Порядок является дополнением к Правилам. В случае выявления разногласий между положениями Правил и настоящим Порядком, положения Порядка будут иметь приоритет.
3. Во всем, что не урегулировано настоящим Порядком, Правилами, а также договорами и соглашениями участников электронного документооборота участники руководствуются действующим законодательством Российской Федерации.
4. Описание атрибутов Сертификатов, позволяющие отнести Сертификат, выданный УЦ, к какому-либо Классу, либо признать его Технологическим сертификатом, приведены в Приложении № 5 к настоящему Порядку.
5. Сертификаты Классов 2, 3 и 4, изготовленные УЦ в порядке и на условиях настоящего Порядка, предназначены для обеспечения электронного документооборота исключительно в рамках правил Системы.

4. Деятельность Удостоверяющего центра

1. УЦ изготавливает Сертификаты и Технологические сертификаты в форме ЭД, устанавливает сроки действия Сертификатов, Технологических сертификатов и предоставляет возможность получения копий Сертификатов и Технологических сертификатов в виде документов на бумажных носителях. УЦ может изготавливать Ключевые носители, содержащие Ключи ЭП, Сертификаты, которые после осуществления предусмотренных правилами Системы процедур, позволяют формировать ЭП.
2. УЦ ведет реестр Сертификатов и Технологических сертификатов, обеспечивает его актуальность и возможность доступа к нему участников информационных систем. Сертификаты и Технологические сертификаты, созданные УЦ, подлежат внесению УЦ в реестр Сертификатов и Технологических сертификатов не позднее даты начала действия Сертификата и Технологического сертификата.
3. УЦ также может выполнять функции Агента по проверке документов Клиентов, предусмотренные разделами 6, 7 настоящего Порядка.
4. Срок действия Сертификата Класса 2,3,4 составляет один год с момента его создания УЦ.
5. УЦ не несет ответственности за любые убытки, которые могут возникнуть у Клиентов, Владельцев сертификатов и иных лиц в связи с использованием Сертификатов, Технологических сертификатов, Криптографических ключей, в том числе убытков, связанных с неправомочным использованием. Все риски, связанные с использованием Сертификатов, Технологических сертификатов, Криптографических ключей несут клиенты, Владельцы сертификатов.
6. УЦ проверяет уникальность Ключей проверки ЭП в реестре Сертификатов и Технологических сертификатов.
7. УЦ осуществляет по обращениям участников электронного взаимодействия проверку Электронных подписей.
8. УЦ осуществляет иную связанную с использованием ЭП деятельность.

5. Порядок создания сертификатов

5.1. Для целей участия в Системе Клиенту необходимо сформировать Электронную подпись. Электронная подпись может быть сформирована для Клиента одним из следующих способов:

* Клиентом самостоятельно в соответствии с разделом 7 настоящего Порядка;
* Агентом в присутствии Клиента при самостоятельном обращении Клиента в Банк в порядке, предусмотренном разделом 6 настоящего Порядка.
1. Порядок создания Сертификатов Агентом УЦ
	1. Изготовление Сертификатов осуществляется на основании Заявления Клиента, поданного им Агенту.

Заявление содержит сведения, необходимые для проверки информации о Клиенте в соответствии с Классом запрашиваемого Клиентом Сертификата и передачи Клиенту сообщений. Заявление формируется в соответствии с типовой формой (Приложение №1 для Клиента - физического лица или Приложение №2 для Клиента - сотрудника юридического лица) и подписывается собственноручно Клиентом или его уполномоченным лицом. Содержащиеся в Заявлении сведения подтверждаются предъявлением в Банк соответствующих документов (для физических лиц – паспорт, для представителей юридических лиц – паспорт, а также письменный документ, заверенный подписью руководителя и печатью организации, подтверждающий право представителя действовать от имени данной организации).

Проверку предоставленных Клиентом сведений производит Агент. Проверка производится в соответствии с Классом Сертификата. По требованию УЦ Агент обязан направить УЦ заверенную копию Заявления Клиента с отметкой Агента о его принятии, а также заверенные копии документов, представленных Клиентом Агенту.

* 1. Получив Заявление и проверив данные Клиента в соответствии с п.6.1, Агент формирует запрос на создание Сертификата. Запрос формируется в виде ЭД, подписанного ЭП Агента и направляется УЦ.
	2. Создание Сертификатов для Клиентов осуществляется УЦ в течение 3 (Трех) рабочих дней с момента получения от Агента электронного запроса в соответствии с п. 6.2.
	3. При изготовлении Сертификатов всегда проверяется уникальность Идентификаторов владельцев сертификатов (DN), принадлежащих разным Владельцам сертификатов, и Открытых ключей в реестре и архиве УЦ. Программно-аппаратные средства УЦ исключают возможность изготовления одинаковых Сертификатов. При изготовлении Ключевых носителей УЦ самостоятельно формирует уникальный Идентификатор владельца сертификата (DN) и присваивает его созданному Сертификату.
	4. УЦ предоставляет Агенту созданные по Заявлению/запросу Агента Сертификаты для Агента/Клиентов в форме ЭД.
	5. Агент при выдаче Криптографических ключей получает от Клиента распечатанный на бумажном носителе Акт приёма-передачи Сертификата Клиента согласно Приложению №3 для Клиента - физического лица или Приложению №4 для Клиента - сотрудника юридического лица в двух экземплярах, с проставленной в Акте собственноручной подписи Клиента или уполномоченного лица Клиента. Второй экземпляр Акта приема-передачи на бумажном носителе хранится у Агента. По требованию УЦ Агент обязан направить УЦ заверенную копию Акта. Направление заверенной копии осуществляется Агентом за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от УЦ. В случае не направления вышеуказанного Акта в предусмотренный срок, УЦ вправе приостановить деятельность такого Агента по формированию запросов на создание Сертификатов и их выдачи Клиентам, письменно уведомив об этом Агента.
	6. По запросу Клиента Агент может предоставить Клиенту Ключевые носители, созданные УЦ, что определяется в соглашении между Клиентом и Агентом.
	7. 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 настоящим разделом. Все риски, связанные с невозможностью использования Сертификата в связи с изменением данных, идентифицирующих Владельца сертификата, несет Владелец сертификата.
	8. В случае, если Владелец сертификата обладает действующим (не утратившим силу) Сертификатом, возможно создание нового Сертификата по удалённому обращению Владельца сертификата в порядке, определённом разделом 8 настоящего Порядка.
1. Порядок создания Сертификатов по удаленному обращению Клиентом
	1. Создание Клиентом Сертификатов по удаленному доступу осуществляется в следующем порядке.
		1. Клиенту необходимо выполнить настройку рабочего местаКонтент страницы
* согласно «Инструкции по настройке браузеров для работы в Интернет-Банке» по следующему электронному адресу: https://faktura.ru/Support/Pages/default.aspx в разделе «Пользователям системы» перейти по ссылке: 1. Настроить компьютер для работы в системе.
	+ 1. Ознакомиться с инструкцией «Дистанционная схема работы УЦ для пользователей», размещенной по следующему электронному адресу: <https://faktura.ru/Support/Pages/download-insructions.aspx>.
		2. Отправку запроса и сохранение Сертификата необходимо осуществлять с использованием браузера Internet Explorer.
		3. Клиент обращается на страницу сервера УЦ по адресу: https://ca.faktura.ru/ca/new-certificate?agentId=4862, предназначенную для выдачи Сертификата класса 2. После заполнения полей формируется Закрытый ключ и Заявление на выдачу Сертификата.
		4. Заявление формируется в соответствии с типовой формой (Приложение №1 для Клиента - физического лица или Приложение №2 для Клиента - сотрудника юридического лица) и подписывается собственноручно Клиентом или его уполномоченным лицом. Запросу автоматически присваивается идентификатор - уникальный номер запроса (далее – УНЗ).
		5. Клиент сообщает Агенту УНЗ, предоставляет в Банк заполненное Заявление на выдачу Сертификата. Содержащиеся в Заявлении сведения подтверждаются предъявлением соответствующих документов (для физических лиц – паспорт, для представителей юридических лиц – паспорт, а также письменный документ, заверенный подписью руководителя и печатью организации, подтверждающий право представителя действовать от имени данной организации). Если Клиент в течение 30 (тридцати) дней с момента создания запроса не предоставляет письменное Заявление, то запрос аннулируется.
		6. Если данные корректны, Агент подтверждает запрос в Системе.
		7. После подтверждения запроса, Системой на Email Клиента, указанный при отправке запроса, направляется письмо со ссылкой для сохранения Сертификата (публичной части ключа).
		8. Клиент переходит по ссылке, указанной в письме, и сохраняет Сертификат. ВАЖНО: необходимо сохранить Сертификат в папку, в которой находится файл Закрытого ключа prv\_key.pfx, созданный при отправке запроса на Сертификат.
		9. После сохранения Сертификата, Клиент распечатывает два экземпляра Акта приема-передачи, подписывает и передает Агенту на бумажном носителе.

7.2. Порядок создания Сертификата по удаленному доступу Клиента, прописанный в разделе 7 настоящего Порядка, может применяться как при первичном, так и при последующем создании Сертификата при условии, что срок действия последнего из использованных Клиентом Сертификатов истек.

1. Порядок создания Сертификатов по удалённому обращению Клиента,

уже являющего Владельцем сертификата

* 1. Создание Сертификата Клиентом, уже являющимся Владельцем Сертификата, срок действия которого не истек, осуществляется в следующем порядке.
		1. Клиент обращается на страницу УЦ, предназначенную для обновления Сертификатов по адресу: https://ca.faktura.ru/ca/renew-certificate и создает запрос на обновление Сертификата. Ознакомиться с руководством пользователя «Дистанционное получение и обновление сертификата» можно на сайте Банка, либо скачать инструкцию «Дистанционная схема работы УЦ для пользователей» по следующему электронному адресу: <https://faktura.ru/Support/Pages/download-insructions.aspx>
		2. Клиент подписывает запрос на новый Сертификат действующим Ключом ЭП. Идентификаторы владельца сертификата нового и действующего Сертификата должны совпадать.
		3. Заверенный Клиентом запрос на новый Сертификат автоматически передается в Системе УЦ. Запрос равнозначен Заявлению Клиента на выдачу Сертификата, заверенному собственноручной подписью Клиента или уполномоченного лица Клиента.
		4. Подтверждением того, что Система успешно приняла запрос Клиента на обновление Сертификата, является присвоение ему уникального номера запроса (далее – УНЗ). Клиент сообщает по телефону Агенту УНЗ.
	2. В случае если срок действия Сертификата Клиента истек, Клиент получает новый Сертификат подписи в соответствии с разделами 6 или 7 настоящего Порядка.
	3. Агент получает на e-mail из Системы УЦ уведомление о зарегистрированном запросе на новый сертификат и после сверки УНЗ, полученного по телефону от Клиента, подтверждает выдачу нового Сертификата в Системе.
	4. УЦ изготавливает новый Сертификат по запросу Клиента. Класс нового Сертификата совпадает с Классом действующего Сертификата Клиента.
	5. Агент получает Акт приёма-передачи нового Сертификата Клиента в Системе в электронном виде.
	6. Агент заверяет Акт приёма-передачи нового Сертификата Клиента ЭП и передаёт его УЦ в Системе в электронном виде, подтверждая тем самым выдачу нового Сертификата Клиенту.
	7. После подтверждения запроса со стороны Агента на e-mail, который был указан в запросе на обновление сертификата, поступит письмо, содержащее ссылку для сохранения сертификата.
	8. При переходе по ссылке откроется страница для сохранения Cертификата. Клиент получает заверенный Агентом Акт приёма-передачи нового Сертификата от Системы в электронном виде.
	9. Клиент заверяет действующей ЭП Акт приёма-передачи нового Сертификата и передаёт Акт УЦ по Системе в автоматическом режиме.
	10. Клиент получает новый Сертификат от Системы в автоматическом режиме.
	11. Сертификат помещается УЦ в реестр Сертификатов.
	12. Агент Акт не хранит, так как Акт приёма-передачи формируется в электронном виде и сохраняется УЦ.
	13. Агент может отказаться от подтверждения выдачи нового Сертификата Клиента, при этом Агент или УЦ направляет Клиенту сообщение об отказе.
1. Срок и порядок хранения Сертификатов в Удостоверяющем Центре
	1. Срок хранения Сертификатов в УЦ после прекращения действия определяется законодательством.
	2. По истечении указанного срока хранения Сертификат исключается из реестра и переводится в режим архивного хранения. Срок архивного хранения определяется Правилами.

Приложение № 1 к Порядку получения ключей электронной подписи клиентами ООО КБ «Металлург»

 АГЕНТУ Удостоверяющего центра «AUTHORITY»

 ООО КБ «Металлург»

 / в Удостоверяющий центр «AUTHORITY»

**ЗАЯВЛЕНИЕ НА ВЫДАЧУ CЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ**

Прошу Удостоверяющий центр «AUTHORITY» изготовить и выдать мне *Сертификат ключа проверки электронной подписи* (*Класс Сертификата*) для физического лица с параметром *Идентификатора владельца сертификата*:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (ФИО / псевдоним *Клиента*). Уникальный номер запроса (только для удаленной выдачи):\_\_\_\_\_\_\_\_\_.

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

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

|  |  |
| --- | --- |
| Реквизиты Клиента: |  |
| ФИО |  |
| Контактный телефон |  |
| E-mail |  |
| Настоящим соглашаюсь с обработкой своих персональных данных ЗАО «Центр Цифровых сертификатов» и признаю, что персональные данные, заносимые в Сертификаты, относятся к общедоступным персональным данным. \_\_\_\_\_\_\_\_(подпись Клиента)/\_\_\_\_\_\_\_\_(Ф.И.О. Клиента) |

принято *Агентом Удостоверяющего центра / Удостоверяющим центром*:

ООО КБ «МЕТАЛЛУРГ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(дата)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись уполномоченного лица)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(ФИО уполномоченного лица)

 М.П.

Приложение № 2 к Порядку получения ключей электронной подписи клиентами ООО КБ «Металлург»

 АГЕНТУ Удостоверяющего центра «AUTHORITY»

 ООО КБ «Металлург»

 / в Удостоверяющий центр «AUTHORITY»

**ЗАЯВЛЕНИЕ НА ВЫДАЧУ CЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ**

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать уполномоченному лицу организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(наименование организации), действующ(-ему)(-ей) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, *Сертификат ключа проверки электронной подписи* (*Класс* \_ *Сертификата*) с параметром *Идентификатора владельца сертификата*:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (ФИО \ псевдоним уполномоченного лица организации / наименование \ псевдоним организации). Уникальный номер запроса (только для удаленной выдачи):\_\_\_\_\_\_\_\_\_.

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

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

Реквизиты *Клиента*:

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

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись уполномоченного лица организации)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф.И.О. уполномоченного лица организации)

М.П. (если применимо)

принято *Агентом Удостоверяющего центра / Удостоверяющим центром*:

ООО КБ «МЕТАЛЛУРГ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(дата)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись уполномоченного лица)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(ФИО уполномоченного лица)

Приложение № 3 к Порядку получения ключей электронной подписи клиентами ООО КБ «Металлург»

АКТ ПРИЕМА - ПЕРЕДАЧИ

<Город администратора ключей> <Текущая дата>

<ФИО, введенные при выдаче Сертификата>, именуем(-ый)(-ая) в дальнейшем "Клиент", с одной стороны, и ООО КБ «Металлург» , именуемое в дальнейшем "Агент", в лице <должность и ФИО администратора ключей либо иного уполномоченного сотрудника Банка>, действующ(-его)(-ей) на основании <документ - данные из УЦ>, с другой стороны, в соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY» составили настоящий Акт приема - передачи о следующем:

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

Идентификатор владельца

сертификата CN= , OU= , O= , L= , C=

Номер Сертификата Алгоритм подписи

Заверен

Годен с

Годен до

Алгоритм Ключа проверки

электронной подписи

Ключ проверки электронной подписи

Алгоритм отпечатка

Отпечаток

2. Обязательства Агента перед Клиентом выполнены в точном соответствии с Правилами
работы Удостоверяющего центра «AUTHORITY», претензий у Клиента не имеется.

От Агента

 **\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Дата подписи)

М.П. От Клиента

**\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_**

(Подпись)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Дата подписи)

Приложение № 4 к Порядку получения ключей электронной подписи клиентами ООО КБ «Металлург»

АКТ ПРИЕМА - ПЕРЕДАЧИ

<Город администратора ключей > <Текущая дата>

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 ООО КБ «Металлург», именуемое в дальнейшем "Агент", в лице <должность и ФИО администратора ключей либо иного уполномоченного сотрудника Банка>, действующ(-его)(-ей) на основании <документ - данные из УЦ>, с другой стороны, в соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY» составили настоящий Акт приема - передачи о следующем:

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

Идентификатор владельца

сертификата CN= , OU= , O= , L= , C=

Номер Сертификата Алгоритм подписи

Заверен

Годен с

Годен до

Алгоритм Ключа проверки

электронной подписи

Ключ проверки электронной подписи

Алгоритм отпечатка

Отпечаток

2. Обязательства Агента перед Клиентом выполнены в точном соответствии с Правилами
работы Удостоверяющего Центра «AUTHORITY», претензий у Клиента не имеется.

От Агента

 **\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Дата подписи)

М.П.

От Клиента

**\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_**

(Подпись)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Дата подписи)

М.П. (если применимо)

Приложение № 5 к Порядку получения ключей электронной подписи клиентами ООО КБ «Металлург»

В Системе действуют Сертификаты трех классов:

– Класс 2 и Класс 3 - при создании Сертификата произведена проверка с предъявлением соответствующих документов, аналогичная проверке при открытии банковского счета, а также проверка на уникальность Идентификатора владельца сертификата таким образом, чтобы Идентификаторы владельцев сертификатов данного Класса, принадлежащие разным Владельцам сертификатов, были уникальны в рамках УЦ;

– Класс 4 - при создании Сертификата осуществляется проверка документов и прочей информации в соответствии с порядком, определяемом Удостоверяющим центром в каждом конкретном случае.

Атрибутом Сертификата, позволяющим отнести Сертификат, выданный УЦ, к какому либо Классу Системы, либо признать его Технологическим сертификатом, является поле с именем сертификата УЦ, которым подписан данный Сертификат или Технологический сертификат.

Соответствие атрибута и Класса выданного Сертификата по терминологии Системы:

|  |  |
| --- | --- |
| Класс Сертификата СИСТЕМЫ | Значение атрибута |
| Класс 2 | CN = Class 2 CA |
| O = Center of Financial Technologies |
|  | C = RU |
| Класс 3 | CN = Class 3 CA |
| O = Center of Financial Technologies |
|  | C = RU |
| Класс 4 | CN = Class 4 CA |
| O = Center of Financial Technologies |
|  | C = RU |

Значение атрибутов Технологических сертификатов:

Значение атрибута

CN = Common 1 CA

O = Center of Financial Technologies

C = RU

CN = Class 1 CA

O = Center of Financial Technologies C = RU