

УТВЕРЖДАЮ

Председатель Правления
ОАО «Газнефтьбанк»

Ведменский А.А.

А.А. Ведменский 2015 г.



**ПРАВИЛА ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ПО СИСТЕМЕ
«ИНТЕРНЕТ-БАНК» В ОАО «ГАЗНЕФТЬБАНК»**

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная цифровая подпись (Электронная подпись) - обязательный реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в электронном документе информации.

Электронный документ - электронное сообщение, распоряжение о переводе денежных средств, заверенное Электронной цифровой подписью, в котором информация представлена в электронно-цифровой форме.

Ключ - общее название пары взаимосвязанных секретного и открытого ключей.

Открытый ключ – ключ проверки ЭЦП или открытый ключ шифрования.

Секретный ключ – последовательность символов, известная владельцу Сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств ЭЦП.

Сертификат ключа проверки ЭЦП (Сертификат ключа подписи) - электронный документ или документ на бумажном носителе, выданный Аккредитованным удостоверяющим центром или доверенным лицом Аккредитованного удостоверяющего центра и подтверждающий принадлежность ключа проверки ЭЦП владельцу Сертификата ключа проверки ЭЦП.

Аккредитованный удостоверяющий центр (Удостоверяющего Центра «AUTHORITY») - Закрытое акционерное общество «Центр Цифровых Сертификатов», ИНН 5407187087, место нахождения: 630055, г. Новосибирск, ул. Шатурская, д. 2.

Инструкция по созданию ключа - порядок действий по генерации ключа и получению сертификата. "Инструкция по созданию ключа на внешнем носителе" и размещена в информационно-телекоммуникационной сети «Интернет» по адресу: <http://www.gazneftbank.ru>.

Средства криптографической защиты информации - 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.

Владелец сертификата ключа проверки ЭП (Владелец сертификата ключа подписи) - физическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки ЭП и которое владеет соответствующим Ключом ЭП, позволяющим с помощью средств ЭП создавать Электронную подпись в Электронных документах (подписывать Электронные документы).

Клиент - юридическое лицо или индивидуальный предприниматель, заключивший с Банком Соглашение.

Сотрудник Клиента - физическое лицо, на которого Клиентом оформлено Заявление на доступ к системе "ИНТЕРНЕТ-БАНК"

Клиентское рабочее место – индивидуальный комплекс технических и программных средств Клиента, обеспечивающий подготовку, редактирование, подписание, отправку, поиск, получение и печать ЭД и справочной информации при взаимодействии с Банком.

Ключевой носитель - информационный (материальный) носитель, содержащий ключ либо предназначенный для записи ключа.

Компрометация ключа - утрата доверия к тому, что используемый секретный ключ недоступен третьим лицам либо утеря ключевой информации вследствие программно- аппаратного сбоя. К событиям, связанным с компрометацией ключа, относятся, включая, но не ограничиваясь, следующие:

- утрата ключевого носителя;
- утрата ключевого носителя с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- смена руководителя организации
- утрата ключей от сейфа в момент нахождения в нем ключевого носителя;
- временный доступ третьих лиц к ключевому носителю;

- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к ключу третьих лиц
- Счет** - счет Клиента, открытый на основании Договора банковского счета.

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сервис (Система "ИНТЕРНЕТ- БАНК") - Сервис "FAKTURA.RU".

Банк - ОАО «Газнефтьбанк».

УЦ - Аккредитованный удостоверяющий центр.

Соглашение - Соглашение об использовании системы «ИНТЕРНЕТ-БАНК».

СКЗИ - Средства криптографической защиты информации.

Правила - «Правила аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"» ОАО «Газнефтьбанк».

ЭД - электронный документ.

ЭЦП (ЭП) - электронная цифровая подпись.

СЕРТИФИКАТ - сертификат ключа проверки ЭЦП (сертификат ключа подписи).

3. ПРЕДМЕТ ДОГОВОРА

3.1. Настоящие Правила обмена электронными документами по системе «Интернет-Банк» устанавливают порядок обслуживания Банком Клиентов с использованием Системы в целях предоставления услуг по Дистанционному банковскому обслуживанию и определяют возникающие в этой связи права, обязанности и ответственность Сторон.

3.2. Правила являются типовым формуляром Банка для всех Клиентов и определяют положения договора присоединения, заключаемого между Банком и Клиентом.

3.3. Заключение Договора осуществляется путем присоединения Клиента к настоящим Правилам в целом в соответствии со статьей 428 Гражданского кодекса Российской Федерации и производится путем акцепта Банком (Аккредитации Клиента в Системе) оферты Клиента (поданного в Банк **Заявления на доступ к системе «Интернет-Банк»** на бумажном носителе, составленного по форме **Приложения 1** к настоящим Правилам). Права и обязанности Сторон по настоящему Договору возникают с момента заключения Договора. Моментом заключения Договора является дата проставления Банком отметки о принятии Заявления Клиента о присоединении к Правилам обмена электронными документами по системе «Интернет-Банк» в ОАО «Газнефтьбанк».

3.4. Банк осуществляет Аккредитацию Клиента в Системе, а Клиент использует Систему обмена Электронными документами Faktura.ru, позволяющую Клиенту осуществлять оперативное управление своими счетами в Банке. Банк, как Расчетный Банк Системы, предоставляет Клиенту следующие услуги:

- прием от Клиента с использованием Системы распоряжений о перечислении денежных средств со счета Клиента в виде Электронных документов;
- передача Клиенту с использованием Системы выписок по счету Клиента в виде Электронных документов;
- возможность обмена иными Электронными документами с Банком с использованием Системы.

3.5. С помощью Системы Клиент получает доступ к управлению своими расчетными/текущими счетами в рублях РФ, открытым в Банке на основании Договоров банковского счета, заключенных между Банком и Клиентом.

3.6. В случае приостановления работы Системы или ее элементов, а также в иных случаях невозможности предоставления/получения услуг по п.3.1., обслуживание Клиента производится с использованием расчетных документов на бумажном носителе в порядке, установленном соответствующим Договором банковского счета.

3.7. Электронный документооборот по обмену ЭД между Банком и Клиентом осуществляется в порядке и на условиях, определенных Правилами Корпоративной Информационной Системы «BeSafe» (далее — «КИС «BeSafe»), расположенных на веб-сервере по адресу www.besafe.ru. (далее — «правила Системы» или «Правила КИС «BeSafe»), а так же к Правилам работы Удостоверяющего Центра «Authority».

4. АККРЕДИТАЦИЯ В СЕРВИСЕ

4.1. Документооборот в Сервисе доступен Клиенту только после выполнения им всех следующих действий:

- наличие клиентского рабочего места, отвечающего требованиям (Приложение №3);
- выполнения всех необходимых действий для генерации ключа (Инструкция по созданию ключа);
- получения Банком Заявления на выдачу сертификата (Приложение №7), Акта приема-передачи сертификата (Приложение №8), Заявления на доступ к системе "ИНТЕРНЕТ-БАНК" (Приложение №1), подписанных Клиентом;
- Заявление на подключение уведомлений (Приложение №2) - при необходимости;

4.2. В соответствии с Инструкцией по созданию ключа и правил работы Удостоверяющего Центра «AUTHORITY», сотрудник Клиента самостоятельно создает **СЕКРЕТНЫЙ КЛЮЧ** и **СЕРТИФИКАТ** с использованием СИСТЕМЫ на программно-аппаратных комплексах КЛИЕНТА. После создания **СЕКРЕТНОГО КЛЮЧА** и **СЕРТИФИКАТА** стороны подписывают соответствующий Акт о признании ЭЦП, являющийся неотъемлемой частью настоящего Соглашения.

4.3. Как альтернативная возможность получения **КЛИЕНТОМ СЕКРЕТНОГО КЛЮЧА** и **СЕРТИФИКАТА**, сотрудник Клиента самостоятельно создает **СЕКРЕТНЫЙ КЛЮЧ** и **СЕРТИФИКАТ** с использованием СИСТЕМЫ на программно-аппаратных комплексах БАНКА. После создания **СЕКРЕТНОГО КЛЮЧА** и **СЕРТИФИКАТА** стороны подписывают соответствующий Акт о признании ЭЦП, являющийся неотъемлемой частью настоящего Соглашения.

5. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ (ОБНОВЛЕНИЕ СЕРТИФИКАТА)

5.1. Срок действия сертификата составляет 1 год с момента генерации сертификата.

5.2. Не позднее, чем за 15 (пятнадцать) рабочих дней до даты фактического истечения срока действия сертификата сотрудник Клиента обязан произвести действия, направленные на обновление сертификата в соответствии с инструкцией пользователя для корпоративных клиентов, размещенной на сайте <http://www.faktura.ru> в разделе "Настройка и поддержка". Поскольку запрос на новый сертификат и акт приема-передачи сертификата формируются в электронном виде, подписываются действующим ключом, представлять в банк документы на бумажном носителе не требуется.

5.3. Если сотрудник Клиента не произвел своевременно плановую смену ключей, его обслуживание в Сервисе приостанавливается с даты окончания срока действия сертификата (осуществляется автоматическая блокировка просроченных ключей сотрудника Клиента).

5.4. Возобновление обслуживания после автоматической блокировки осуществляется после создания сотрудником Клиента новых ключей в соответствии с п. 4.2-4.3 и представления в Банк Заявления на выдачу сертификата и Акта приема-передачи сертификата, подписанных Клиентом.

6. СМЕНА КЛЮЧЕЙ ВСЛЕДСТВИЕ КОМПРОМЕТАЦИИ

6.1. В случае компрометации ключей Клиент сообщает в Банк о случившемся по телефону или любым другим способом, после чего направляет в банк в двух экземплярах заявление о аннулировании действия ключа ЭЦП (Приложение №6) (далее - «Уведомление»), заверенное печатью и подписью Клиента. Уведомление принимается к исполнению по рабочим дням.

6.2. При получении от Клиента Уведомления на бумажном носителе, сотрудник Банка указывает на бланке Уведомления дату и время его получения и передает Клиенту второй экземпляр уведомления с отметкой времени регистрации.

6.3. Не позднее 2 (двух) часов после получения Банком Уведомления Банк прекращает прием документов, подписанных ЭЦП, сформированной на скомпрометированном ключе. Если Уведомление получено Банком менее, чем за 2 часа до истечения рабочего дня, то срок исполнения Уведомления может быть перенесен на следующий рабочий день.

6.4. Направление Уведомления означает требование Клиента прекратить прием и исполнение любых ЭД, подписанных ЭЦП, сформированных с использованием скомпрометированного ключа.

6.5. Клиент осуществляет действия для генерации/получения новых ключей и оформления сертификата в соответствии с разделом 4.

7. ОБЩИЕ УСЛОВИЯ И ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

7.1. Электронные документы передаются Клиентом с использованием средств Системы, при этом обмен документами на бумажных носителях сторонами не производится, кроме случаев, предусмотренных настоящим договором, в частности при возникновении обстоятельств непреодолимой силы или возможных нарушениях работы Системы, а также в иных случаях, предусмотренных соглашениями между Банком и Клиентом.

7.2. Банк осуществляет платежи на основании расчетных документов в электронной форме при условии соответствия этих документов требованиям законодательства РФ, Договора банковского счета, форматам, установленным Системой, а также наличия корректной ЭЦП.

7.3. Стороны признают, что полученные с помощью Системы электронные документы, заверенные ЭЦП, юридически эквивалентны документам, составленным на бумажном носителе, подписанным уполномоченными лицами и удостоверенным печатью Клиента и являются основанием проведения операций по счету Клиента.

7.4. В случае несоответствия электронного документа требованиям п.7.2. настоящего договора, положений заключенных между сторонами договоров, соглашений, а также в случае выявления угрозы несанкционированного доступа к программно-аппаратным средствам Клиента или его счетам, Банк отказывает в исполнении документа, уведомив Клиента посредством Системы о причинах отказа.

7.5. Прием электронных документов производится Банком круглосуточно. Исполнение расчетных документов осуществляется в соответствии с тарифами Банка на момент исполнения этих документов. Исполнение документов, поступивших в Банк, в операционное время, исполняются Банком в тот же день, документы, поступившие и принятые позже указанного времени, на следующий рабочий день.

7.6. Стороны признают, что способы защиты и обеспечения целостности информации, средства аутентификации и авторизации, применяемые Системой при передаче электронных документов, достаточны для подтверждения авторства и подлинности документов, и обязуются выполнять режим обеспечения безопасности, установленный правилами Системы. К исполнению документы принимаются только после проверки подлинности всех ЭЦП электронных документов.

7.8. Стороны признают, что срок действия Сертификата составляет один календарный год с даты его выдачи. Продление срока действия Сертификата осуществляется путем выдачи нового Сертификата с обязательной сменой ключей ЭЦП. Выдача нового Сертификата производится по инициативе Клиента не позднее 15 календарных дней до момента окончания срока действия действующего Сертификата. Исполнение сторонами обязательств по настоящему договору приостанавливается с момента окончания срока действия Сертификата и до момента оформления Клиенту нового Сертификата. В течение этого срока стороны не вправе проводить в Системе какие-либо операции, а Банк прекращает прием электронных документов.

7.9. Стороны также признают, что:

- при любом изменении электронного документа, совершенном после его подписания электронной цифровой подписью одной из сторон, электронная цифровая подпись становится некорректной;
- знание информации, которая передается между сторонами по каналу связи Системы, не приводит к компрометации закрытых ключей ЭЦП сторон;
- подделка электронной цифровой подписи участника Системы, т.е. создание корректной электронной цифровой подписи, невозможна без знания закрытого ключа ЭЦП;
- созданный в единственном экземпляре в рамках настоящего договора закрытый ключ ЭЦП Клиента уникален, создание дубликата закрытого ключа ЭЦП возможно только Клиентом или при нарушении Клиентом условий хранения и/или использования закрытого ключа ЭЦП, предусмотренных настоящим договором;

- каждый участник Системы несет ответственность за сохранение в тайне своих закрытых ключей ЭЦП, паролей, за правильность заполнения и оформления электронных документов и за действия своего персонала при работе с Системой. Правильность оформления и заполнения полей электронного документа проверяется ответственным должностным лицом Клиента. Ответственность за передачу ошибочного электронного документа несет Клиент.
- присоединяясь к настоящим Правилам Клиент соглашается с тем, что привлечение Банком оператора и использование удостоверяющего центра для осуществления операций с использованием Системы (в частности, при формировании и передаче документов через процессинговый центр оператора) не является нарушением Банком банковской тайны.

7.10. Стороны определили, что в течение срока действия настоящих Правил допускается временное приостановление Банком/Оператором работы Системы по техническим причинам, но не более чем на четыре часа в сутки.

8. ПОРЯДОК РАСЧЕТОВ

8.1. Клиент обязуется оплачивать Банку комиссионное вознаграждение за оказываемые Банком услуги в порядке и в размерах, установленных Тарифами и настоящими Правилами, а также возмещать другие расходы, понесенные Банком и связанные с обслуживанием Клиента в Системе (стоимость телефонных переговоров, факсимильных сообщений и почтовых отправок, иные расходы). Для этого Клиент поручает Банку списывать указанные комиссионные вознаграждения и расходы без дополнительного распоряжения Клиента с любых Счетов Клиента, что является заранее данным акцептом.

8.2. Клиент обязуется обеспечить наличие на расчетном счете денежных средств в сумме, достаточной для оплаты услуг Банка на условиях списания по требованию Банка. При отсутствии на расчетном счете денежных средств, либо их недостаточности, при списании по требованию Банка Клиент обязан оплатить услуг и Банка не позднее последнего рабочего дня текущего месяца, при этом днем оплаты считается дата поступления денежных средств на счет Банка.

8.3. Банк вправе в одностороннем порядке изменять размер стоимости любых оказываемых услуг. В случае несогласия с новыми Тарифами Клиент вправе в одностороннем порядке расторгнуть настоящий Договор, письменно уведомив об этом Банк.

8.4. В случае неисполнения Клиентом обязательств по уплате услуг в рамках данного Договора и Договора банковского счета, Банк вправе приостановить работу Клиента с использованием Системы. В случае неисполнения указанных обязательств более 3-х месяцев подряд, Банк вправе расторгнуть настоящий Договор, письменно уведомив об этом Клиента

9. ПРАВА И ОБЯЗАННОСТИ СТОРОН

9.1. Права Клиента

9.1.1. На основании настоящего договора Клиент вправе с использованием Системы осуществлять расчетные операции по банковскому счету/счетам, открытым в Банке и указанным Клиентом в заявке на подключение Системы иных электронных документов;

9.1.2. Клиент вправе получить выписку о движении денежных средств по его счетам, как с помощью средств Системы, так и на бумажном носителе.

9.1.3. Клиент имеет право обращаться в службу поддержки сервиса "ФАКТУРА.RU" по телефону **8-800-200-92-50**:

- для получения консультаций по работе в Сервисе (в том числе по настройке взаимодействия с бухгалтерскими системами - 1С и т.д.);
- в случае технических ошибок в работе Сервиса;
- Вход в систему;

- Отправка платежных документов;
- Получение, экспорт выписок;
- Доставка SMS уведомлений;
- Загрузка платежей, реестров из 1С.

9.1.4. Клиент имеет право обращаться в Банк:

- по вопросам прохождения платежей, по поводу запросов направленных в почтовых сообщениях;
- для изменения доступа в Сервисе (подключение новых сотрудников, уведомлений, доверенных IP-адресов);
- для уведомления о компрометации ключа.

9.1.5. В течение срока действия настоящего договора Клиент вправе в любое время прекратить передачу документов, а Банк обязан прекратить прием документов с момента поступления соответствующего требования от Клиента. Требование должно быть предоставлено в письменной форме, подписано уполномоченным лицом и заверено печатью Клиента.

9.1.6. Клиент (уполномоченный представитель Клиента) вправе инициировать замену ключей ЭЦП в любой момент до истечения срока их действия.

9.1.7. Для обеспечения более высокого уровня безопасности, Клиент вправе подключить сервис подтверждения платежей по своим счетам одноразовыми паролями через СМС уведомления – «Сервис одноразовых паролей». Стоимость использования данного сервиса определяется тарифами Банка на момент его использования.

9.2. Обязанности Клиента

9.2.1. Клиент обязан самостоятельно контролировать исполнение Расчетных документов и документов валютного контроля, отправленных в Банк с использованием средств Системы, посредством контроля изменений состояния отправленного электронного документа.

9.2.2. Клиент обязан за свой счет поддерживать в рабочем состоянии принадлежащие ему аппаратные и программные средства, в том числе средства антивирусной защиты, используемые для функционирования Системы, а также обеспечить своевременное их обновление.

9.2.3. Клиент обязан соблюдать правила информационной безопасности при использовании Системы (Приложение №4):

- обеспечить хранение материального носителя, содержащего закрытый ключ ЭЦП в месте, исключающем доступ неуполномоченных лиц и/или повреждение материального носителя (сейф, личная запираемая ячейка и т.п.);
- хранить закрытый ключ ЭЦП на сменном носителе (flash-карта, диск, дискета);
- исключить хранение закрытого ключа ЭЦП на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах;
- исключить передачу закрытого ключа ЭЦП и его копий третьим лицам, а так же передачу по телефону, электронной почте или публичным сетям;
- в случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям, должна быть проведена смена ключей ЭЦП, к которым он имел доступ;
- при подозрении несанкционированного доступа третьих лиц к счетам, программно-аппаратным средствам Клиента, копирования или подозрения в копировании ключей третьими лицами, с целью предотвращения финансовых потерь, незамедлительно любым доступным способом проинформировать об этом Банк и инициировать процедуру смены всех потенциально скомпрометированных ключей ЭЦП.

9.2.4. В случае изменения у Уполномоченных лиц Клиента или иных лиц, участвующих в электронном документообороте между Банком и Клиентом в рамках Договора, имени, фамилии, отчества, полномочий или лишения их права работы в Системе немедленно направлять в Банк соответствующее письменное заявление об аннулировании Ключа ЭЦП указанных лиц, составленное по форме Приложения 5 к настоящим Правилам.

9.2.5. При включении новых лиц в состав Уполномоченных лиц Клиента или иных лиц, участвующих в электронном документообороте между Банком и Клиентом в рамках Договора, представлять в Банк письменное Заявление на доступ к системе «ИНТЕРНЕТ-БАНК», составленное по форме Приложения 1 к настоящим Правилам, документы, удостоверяющие личности, и документы, подтверждающие полномочия указанных лиц на использование аналогов собственноручной подписи (электронной подписи) от имени Клиента (если ранее указанные документы в Банк не представлялись) и провести процедуру аккредитации в соответствии с п.4 настоящих правил.

9.2.6. Клиент гарантирует Банку, что все проводимые им операции по счету с использованием средств Системы носят легитимный характер, не нарушают действующего законодательства РФ, и не связаны с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

9.2.7. В случае подключения сервиса подтверждения платежей по своим счетам одноразовыми паролями через СМС уведомления –«Сервис одноразовых паролей», Клиент при блокировании сим-карты, выхода из строя телефона, подозрений, что телефоном завладел злоумышленник, обязан немедленно любым доступным способом известить об этом Банк.

9.3. Права Банка

9.3.1. В течение всего срока действия настоящего договора Банк вправе в одностороннем внесудебном порядке изменять действующие тарифы. Информирование Клиента об изменении тарифов осуществляется путем размещения соответствующей информации на информационных стендах в операционных залах Банка, на корпоративном Интернет-сайте Банка www.gazneftbank.ru или посредством Системы.

9.3.2. Банк вправе отказать Клиенту в приеме от него распоряжения на проведение операции или приостановить совершение Клиентом операций по счету с использованием средств Системы в случаях и в порядке, установленных ФЗ РФ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" No 115-ФЗ от 07.08.2001г.

9.3.3. На время разрешения спорной ситуации, связанной с исполнением Банком электронного документа Клиента, Банк вправе в одностороннем внесудебном порядке приостановить обслуживание Клиента в Системе с последующим его уведомлением.

9.3.4. При обнаружении Банком признаков (фактов) нарушения требования безопасности, установленных настоящим договором, Банк вправе немедленно приостановить прием электронных документов Клиента, после чего должен любым доступным способом известить об этом Клиента.

9.3.5. Банк имеет право направлять Клиенту с использованием средств Системы рекламные материалы и информационные сообщения об услугах и продуктах Банка.

9.4. Обязанности Банка

9.4.1. Банк обязуется предоставлять Клиенту услуги с использованием Системы согласно п.9.1.1, п.9.1.2 настоящего договора.

9.4.2. Предоставлять Клиенту необходимые рекомендации и методическую помощь в работе с Системой.

9.4.3. По требованию Клиента блокировать в Системе активные открытые ключи ЭЦП Клиента, регистрировать новые открытые ключи ЭЦП, временно блокировать работу Клиента в Системе.

10. ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. Стороны обязуются обеспечивать конфиденциальность сведений о технологии Системы.

10.2. Стороны обязуются формировать и хранить не менее трех лет (а в случае возникновения споров – до их разрешения) архивы:

- всех своих открытых и закрытых ключей ЭЦП;
- всех входящих электронных документов в принятом виде с электронной цифровой подписью;
- всех исходящих электронных документов в исходном виде с электронной цифровой подписью;
- электронных протоколов сеансов обмена информацией.

Стороны несут ответственность за целостность и достоверность этих архивов. Сроки хранения электронных расчетных документов должны соответствовать срокам хранения, установленным для расчетных документов на бумажных носителях. Сроки хранения электронных протоколов определяются Банком.

10.3. Банк не несёт ответственности за ущерб, возникший вследствие:

- некорректного оформления Клиентом электронных документов;
- ошибочно переданных электронных документов Клиентом в Банк;
- несанкционированного доступа посторонних лиц к программно-аппаратным средствам, закрытого ключа ЭЦП, используемых Клиентом для осуществления обмена электронными документами;
- воздействия вредоносного программного обеспечения на программно-аппаратные средства, используемые Клиентом для осуществления обмена электронными документами.

10.4. Ни одна из Сторон не будет нести ответственность за полное или частичное неисполнение своих обязательств по настоящему договору, если неисполнение будет являться следствием обстоятельств непреодолимой силы.

10.5. Если любое из вышеуказанных обстоятельств непосредственно повлияло на исполнение обязательств в сроки, установленные настоящим договором, то эти сроки соразмерно отодвигаются на время действия соответствующего форс-мажорного обстоятельства.

10.6. Сторона, для которой создались условия, при которых исполнение ее обязательств стало невозможным, обязана не позднее 1 (одного) дня направить другой стороне уведомление в письменной форме о наступлении таких условий.

11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Споры, возникающие в связи с исполнением Договора, Стороны обязуются разрешать путем переговоров с учетом принципов добросовестности и взаимного уважения, в соответствии с порядком, установленным настоящим разделом Правил.

11.2. Для рассмотрения спорных ситуаций, связанных с обменом Сторонами ЭД, Клиент передает в Банк в письменном виде претензию с указанием информации о спорном Электронном документе. До подачи в письменном виде претензии Клиент должен убедиться в целостности своего программного обеспечения, отсутствии вредоносных программ (компьютерных вирусов), неизменности используемой ключевой информации, а также отсутствии несанкционированных действий Уполномоченных лиц Клиента, использующих Систему «Интернет-Банк», и/или третьих лиц.

11.3. Банк в течение 30 (Тридцати) календарных дней с даты получения претензии Клиента рассматривает претензию Клиента и, в зависимости от принятого решения, либо удовлетворяет претензию Клиента, либо передает Клиенту письменное заключение о необоснованности его претензии, подписанное уполномоченным работником Банка.

11.4. В случае несогласия с заключением Банка по предъявленной Банку претензии Клиент направляет в Банк письменное уведомление о своем несогласии с требованием о формировании экспертной комиссии для рассмотрения спора.

11.5. Рассмотрение претензии производится в каждом конкретном случае в зависимости от содержания претензии, в соответствии с действующим законодательством и правилами Банка.

11.6. В случае несогласия с решением по претензии любая из Сторон вправе передать спор на рассмотрение в соответствии с законодательством Российской Федерации в Арбитражный суд Саратовской области.

12. СРОК ДЕЙСТВИЯ ДОГОВОРА. ПРЕКРАЩЕНИЕ ДОГОВОРА

12.1. Договор вступает в силу с момента его заключения Сторонами, с учетом п. 3.3. Договора, и действует до 31 декабря текущего года. В случае если ни одна из Сторон письменно не уведомила другую Сторону в срок не позднее, чем за 30 (тридцать) календарных дней до окончания срока действия Договора о своем намерении расторгнуть Договор в одностороннем порядке, действие Договора считается продленным на каждый следующий календарный год.

12.2. Договор может быть расторгнут досрочно в одностороннем порядке по требованию одной из Сторон в следующем порядке:

- В случае расторжения Договора по инициативе Банка, последний письменно уведомляет об этом Клиента не позднее, чем за 15 (пятнадцать) календарных дней до момента предполагаемого расторжения Договора посредством направления уведомления по почтовому адресу, указанному Клиентом в Заявлении о присоединении к Правилам (в случае, если Клиент письменно извещал Банк в течение действия Договора об изменении адреса – по последнему из указанных адресов), либо путем передачи уведомления Клиенту, при посещении им Банка, либо посредством направления Банком сообщения Клиенту в виде Электронного документа по Системе. Обязательства Банка по приему и исполнению ЭД с использованием Системы считаются прекращенными с даты и времени, указанных в уведомлении.
- В случае расторжения Договора по инициативе Клиента, последний обязан передать в Банк письменное Заявление о расторжении Договора дистанционного банковского обслуживания, составленного по форме Приложения №6. Договор считается расторгнутым с даты получения Банком указанного заявления при условии отсутствия у Клиента обязательств по погашению перед Банком задолженности по Договору. При наличии указанных обязательств по погашению задолженности перед Банком Договор считается расторгнутым с момента исполнения Клиентом обязанности по оплате указанной задолженности.

12.3. Все надлежащим образом оформленные ЭД Клиента, направленные Клиентом в Банк до момента получения Банком Заявления о расторжении Договора дистанционного банковского обслуживания, подлежат исполнению Банком в соответствии с условиями настоящих Правил. С момента получения Банком заявления Клиента о расторжении Договора Банк прекращает прием и завершает исполнение ранее принятых ЭД Клиента.

12.4. Действие Договора также считается прекращенным в день наступления любого из следующих условий и при отсутствии задолженности Клиента перед Банком по Договору:

- отсутствие у Клиента в Банке Счетов, расчеты по которым могут осуществляться путем направления в Банк ЭД с использованием Системы и/или прекращение действия договоров (соглашений), предусматривающих возможность обмена информацией с использованием Системы;
- окончание срока действия последнего Ключа ЭЦП Уполномоченного лица Клиента и непредставление Клиентом в течение 6 (шести) месяцев после этого в Банк документов о формировании и регистрации нового Ключа ЭЦП;
- неисполнение Клиентом обязанности по хранению Ключа.

О наступлении событий, повлекших прекращение Договора, и отсутствии у Банка обязательств перед Клиентом Банк письменно извещает Клиента.

12.5. В случае наличия оснований, указанных в пунктах 12.4 настоящих Правил, и погашения задолженности Клиента перед Банком, действие Договора считается прекращенным с момента погашения указанной задолженности.

12.6. Расторжение Договора (прекращение действия Договора) не влечет прекращения обязательств по иным договорам (соглашениям), заключенным между Клиентом и Банком.

13. УЧЕТ И ХРАНЕНИЕ ЭД

13.1. Учет ЭД, отправленных через Сервис, осуществляется оператором Сервиса ЗАО «Биллинговый центр» (ИНН 5401152049, местонахождение: 630128, г. Новосибирск, ул. Инженерная, д. 4а).

13.2. Архивное хранение ЭД осуществляется в соответствии с действующим законодательством РФ, а также Правилами работы сервиса «ФАКТУРА.RU».

ЗАЯВЛЕНИЕ НА ДОСТУП К СИСТЕМЕ «ИНТЕРНЕТ-БАНК»

Прошу предоставить доступ к системе "ИНТЕРНЕТ-БАНК", подключить Сертификат:
ДЛЯ КЛИЕНТА (ЗАПОЛНЯЕТСЯ ПЕЧАТНЫМИ БУКВАМИ)

Наименование Клиента _____
ИНН/КПП _____
ОГРН _____
Адрес местонахождения: _____
Контактная информация
(телефон/факс): _____
Номер(а) счета(ов): _____

Настоящим заявляем о присоединении вышеуказанного Клиента к действующей редакции Правил обмена Электронными документами по Системе «Интернет-Банк» в ОАО «Газнефтьбанк» (далее – Правила) в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации, и подтверждаем, что все положения Правил нам известны и разъяснены в полном объеме, включая ответственность Сторон, Тарифы ОАО «Газнефтьбанк» и порядок внесения в Правила изменений и дополнений.

Настоящим подтверждаем ознакомление с «Мерами безопасности при работе с Системой «Интернет-Банк», размещенными на сайте www.gazneftbank.ru.

Настоящим просим зарегистрировать в качестве Владельцев ЭЦП следующих Уполномоченных лиц Клиента:

№ п/п	Фамилия, Имя, Отчество	Паспортные данные	Уровень доступа

Вместе с заявлением представлены (указываются, если ранее данные документы в Банк не представлялись):

- документы, удостоверяющие личность Уполномоченных лиц Клиента (оригиналы или нотариально заверенные копии) на _____ листах.
- документы, подтверждающие право Уполномоченных лиц Клиента использовать аналог собственноручной подписи (электронную подпись) от имени Клиента (оригиналы или заверенные в установленном Банком порядке копии с предоставлением оригиналов для сверки) на _____ листах.

С обработкой персональных данных в соответствии с требованиями Федерального Закона № 152-ФЗ от 27.07.2006г. "О персональных данных" согласен(на):

_____ (подпись владельца сертификата).

_____ (подпись владельца сертификата)

(должность руководителя Клиента)

(подпись)

(фамилия, имя, отчество полностью)

Главный бухгалтер

(подпись)

(фамилия, имя, отчество полностью)

« ____ » _____ 20 ____ г.

М.П.

Заполняется Банком

Заявление зарегистрировано в Банке « ____ » _____ 20 ____ г., присвоен № _____

Работник Банка:

(подпись)

(фамилия, инициалы)

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ УВЕДОМЛЕНИЙ

Наименование Клиента _____
 ИНН/КПП _____
 Перечень счетов организации для _____
 подключения уведомлений _____

В рамках соглашения об использовании системы «интернет-банк» прошу осуществлять уведомления по следующему(им) телефону(ам) / электронному(ым) адресу(ам) сотрудника(ов):

Внимание! Указываются только сотрудники организации, зарегистрированные в сервисе

ФИО Сотрудника организации	
----------------------------	--

Мобильный телефон	+7												
E-mail													

С обработкой персональных данных в соответствии с требованиями
 Федерального Закона № 152-ФЗ от 27.07.2006 г. "О персональных данных" согласен(на):

Отметить нужное:

- Прошу установить возможность дополнительного пароля на вход в систему (При входе в систему идентифицируется не только ключ электронной подписи, но дополнительно разовый пароль, высланный на мобильный телефон);
- Уведомлять при входе в систему;
- Уведомлять об отправке платежей в Банк ;

(должность руководителя Клиента)
 _____ / _____ /
(подпись) (фамилия, имя, отчество полностью)

Главный бухгалтер
 _____ / _____ /
(подпись) (фамилия, имя, отчество полностью)

М.П. « ____ » _____ 20 ____ г.

Заполняется Банком
 Заявление зарегистрировано в Банке « ____ » _____ 20 ____ г., присвоен № _____

Работник Банка: _____
(подпись) (фамилия, инициалы)

ТРЕБОВАНИЯ К РАБОЧЕМУ МЕСТУ КЛИЕНТА

1. Операционные системы: Windows 2000/XP/Vista/7/8.
2. Браузер: IE 7.0 и выше (обязательно с поддержкой 128-битного шифрования).
3. Прокси-сервер должен обеспечивать возможность устанавливать исходящие соединения по 443 порту(SSL), а также возможность загружать файлы размером более 1МБ.

Настройки англоязычной версии Internet Explorer:

1. Закладка General: Settings/Check for newer version of stored pages – Automatically
2. Закладка Advanced: Do not save encrypted pages to disk -Checked Use HTTP 1.1 through proxy connection - Checked Use SSL 2.0 - Checked Use SSL 3.0 - Checked
3. Закладка Security Download signed ActiveX controls - Prompt Run ActiveX Controls and plugins - Enable
4. Script ActiveX controls marked safe for scripting - Enable Allow META REFRESH - Enable

Настройки русскоязычной версии Internet Explorer:

1. Закладка Общие Параметры – Проверять наличие обновления сохраненных страниц Автоматически;
2. Закладка Дополнительно SSL 2.0 – Checked SSL 3.0 – Checked Использовать HTTP 1.1 через прокси-соединения - Checked Не сохранять зашифрованные страницы на диск – Checked;
3. Закладка Безопасность Выполнять сценарии элементов ActiveX, помеченных как безопасные –Разрешить;
4. Загружать подписанные элементы ActiveX - Предлагать Запуск элементов ActiveX и модулей подключения – Разрешить метаобновление – Разрешить.

Дополнительные настройки браузера Internet Explorer 10/11:

1. Откройте сайт www.faktura.ru в браузере Internet Explorer.
2. Нажмите кнопку «Alt», выберите меню «Сервис», затем «Параметры просмотра в режиме совместимости».
3. Добавьте «faktura.ru», «authority.ru» в список.

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОГО СРЕДСТВА ПЛАТЕЖА

Для безопасного использования сервиса "ФАКТУРА.RU" как электронного средства платежа, Клиент должен следовать следующим рекомендациям:

1. Общие меры безопасности:

- обеспечить постоянную доступность номера мобильного телефона/адреса электронной почты, на которые подключены уведомления, и ежедневно проверять SMS-сообщения/сообщения электронной почты;
- в случае утраты мобильного телефона, незамедлительно заблокировать SIM-карту;
- при получении сообщения в формате SMS либо в электронном формате по электронной почте либо звонка по телефону, Клиент обязан убедиться, что такое сообщение/звонок исходит именно от Банка или уполномоченного им лица;
- при получении сообщений, следует отказаться от выполнения действий, изложенных в сообщениях в следующих случаях:
 - сообщение поступило не от Банка или уполномоченного им лица;
 - сообщение поступило не с официальных телефонных номеров Банка, которые указаны на официальном сайте Банка в сети Интернет;
 - запрашиваемые в сообщении действия требуют срочного ответа Клиента;
 - сообщение требует предоставить, обновить или подтвердить персональную информацию Клиента (например ПИН-код, номер телефона, имя пользователя, пароль, иную ключевую/парольную информацию);
 - сообщение содержит форму для ввода персональной информации Клиента;
 - в сообщении содержится информация, что на счёт Клиента непредвиденно для него поступили денежные средства;
 - в сообщении содержится просьба войти в систему ДБО по указанной ссылке;
 - полученная информация вызывает любые сомнения или подозрение на мошенничество ежедневно в Сервисе проверять состояние всех своих счетов, включая остаток по счету, доступный баланс по счету, операции по счету и незамедлительно уведомлять Банк лично о наличии ошибок, неточностей или возникновении вопросов в отношении информации, содержащейся в Сервисе.
- соблюдать рекомендации по обеспечению безопасности, размещенные на сайте Банка, на сайте Faktura.ru.

2. Рекомендации по обеспечению безопасности при работе в Интернет:

- использовать только лицензионное системное и прикладное программное обеспечение, а так же обеспечить их регулярное обновление;
- применять средства антивирусной защиты и специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение, обеспечивая
- при этом своевременное обновление антивирусных баз, а также осуществлять еженедельную
- антивирусную проверку, а так же проверку после любых действий сторонних лиц, в том числе и технических специалистов;
- исключить возможность посещения интернет-сайтов сомнительного содержания с компьютера, на котором ведется работа в Системе;

- обеспечить защиту от несанкционированного доступа к компьютеру, на котором установлено программное обеспечение Системы, а так же запретить или существенно ограничивать;
- использование любых средств удалённого доступа;
- установить сложные пароли для всех учётных записей, имеющих право входа на компьютер, на котором ведется работа в Системе, а также осуществлять их периодическую смену;
- не использовать Сервис если соединение с сайтом системы ДБО не зашифровано (отсутствует индикация работы браузера в защищенном режиме) или при его посещении возникают ошибки проверки подлинности сертификата;
- не вводите свои средства авторизации на сайтах, адреса которых отличны от <https://faktura.ru>; <https://www.authority.ru>;
- самостоятельно указывайте адрес сайта в соответствующем поле браузера;
- избегайте работы с системой «Интернет-Банк» в публичной среде, такой, как интернет кафе, социальные точки доступа в интернет, компьютеры друзей и тому подобное, а также в присутствии посторонних лиц;
- подключите SMS-уведомление о входе в систему;
- при входе в Сервис необходимо проверять дату и время последнего входа. В случае подозрения на несанкционированный доступ к системе либо компрометацию ключевой/парольной информации, незамедлительно сообщить об этом в Банк своему куратору, а затем лично в письменной форме;
- завершать работу в Сервисе в соответствии с установленными процедурами. Не закрывайте окно браузера, без предварительного выхода из Сервиса. Если Клиент не выполнял вход в Сервис, но при этом получил сообщение о входе, незамедлительно сообщить об этом в Банк своему куратору, а затем лично в письменной форме.

3. Рекомендации по обеспечению безопасности при использовании Сервиса на мобильных устройствах:

- использовать на мобильных устройствах только официальные приложения, предоставленные оператором Сервиса.
- не использовать несанкционированные модификации программного обеспечения мобильных устройств (взлом прошивки, rooting, jailbreaking);
- не использовать мобильные устройства для доступа к полнофункциональной версии Сервиса;

3. Рекомендации по обеспечению безопасности ключевой информации:

- необходимо хранить ключи ЭЦП только на внешних носителях (дискеты, флеш-накопители и др.), а не на жёстких или сетевых дисках компьютера. Не записывать на данный носитель какую либо другую информацию;
- ключевой носитель необходимо извлекать из компьютера каждый раз после завершения использования, а так же не отлучаться от рабочего места во время работы в Системе;
- не допускать использования простых паролей (123456, qwerty, дата рождения, номер телефона и т.п.), а также осуществлять периодическую их смену. Ни в коем случае не записывать пароли на бумажных листках (или в текстовых файлах на компьютере), не оставлять их в легкодоступных местах;
- никому, включая работников Банка, ни при каких условиях не сообщайте пароль на ключ;
- используйте виртуальную клавиатуру при наборе пароля;

- не допускать передачу ключевого носителя кому-либо, в том числе техническим специалистам для проверки работы Системы, настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец ключа ЭЦП обязан лично подключать ключевой носитель к компьютеру и вводить в Систему пароль.

**ЗАЯВЛЕНИЕ
О АННУЛИРОВАНИИ ДЕЙСТВИЯ
КЛЮЧА ЭЦП ДЛЯ РАБОТЫ ПО СИСТЕМЕ «ИНТЕРНЕТ-БАНК»**

Настоящим _____
(наименование Клиента)

(далее – Клиент) просит на основании Договора дистанционного банковского обслуживания, заключенного путем присоединения к условиям Правил обмена Электронными документами по Системе «Интернет-Банк» в ОАО «Газнефтьбанк» на основании Заявления № _____ от «___» _____ 20__ г.

аннулировать действие Ключа ЭЦП:

(фамилия, имя, отчество Уполномоченного лица Клиента)

с «___» _____ 20__ г.

(фамилия, имя, отчество Уполномоченного лица Клиента)

с «___» _____ 20__ г.

(должность руководителя Клиента)

(подпись)

(фамилия, имя, отчество полностью)

Главный бухгалтер

(подпись)

(фамилия, имя, отчество полностью)

«___» _____ 20__ г.

М.П.

Заполняется Банком

Заявление зарегистрировано в Банке «___» _____ 20__ г., присвоен № _____

Работник Банка:

(подпись)

(фамилия, инициалы)

**ЗАЯВЛЕНИЕ
О РАСТОРЖЕНИИ ДОГОВОРА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ПО
СИСТЕМЕ «ИНТЕРНЕТ-БАНК»**

Наименование Клиента _____
ИНН/КПП _____
ОГРН _____
Адрес местонахождения: _____
Контактная информация
(телефон/факс): _____
Номер(а) счета(ов): _____

Настоящим заявляем о расторжении с «___» _____ 20__ г. Договора дистанционного банковского обслуживания, заключенного путем присоединения к условиям Правил обмена электронными документами по Системе «Интернет-Банк» в ОАО «Газнефтьбанк» на основании Заявления № _____ от «___» _____ 20__ г.

(должность руководителя Клиента)

(подпись)

(фамилия, имя, отчество полностью)

Главный бухгалтер

(подпись)

(фамилия, имя, отчество полностью)

«___» _____ 20__ г.

М.П.

Заполняется Банком

Заявление получено в _____ часов _____ минут «___» _____ 20__ г., присвоен № _____

Работник Банка:

(подпись)

(фамилия, инициалы)

**Агенту Удостоверяющего центра «AUTHORITY»
В ОАО «Газнефтьбанк»
/ в Удостоверяющий центр «AUTHORITY»**

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

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

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

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

Реквизиты Клиента: ФИО уполномоченного лица организации	
Наименование организации	
Контактный телефон	
E-mail	

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

_____ (подпись уполномоченного лица организации)

_____ (Ф.И.О. уполномоченного лица организации)
М.П. (если применимо)

принято *Агентом Удостоверяющего центра / Удостоверяющим центром:*

_____ (полное наименование)

_____ (дата)

_____ (подпись уполномоченного лица)

_____ (ФИО уполномоченного лица) М.П.
М.П.

**АКТ ПРИЕМА – ПЕРЕДАЧИ
СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ**

<Город администратора ключей >

<Дата создания акта>

Юридическое лицо < наименование организации, введенное при выдаче Сертификата >, именуемое в дальнейшем "Клиент", представленное своим уполномоченным лицом <ФИО уполномоченного лица, оформившего заявку на сертификат>, с одной стороны, и <Наименование Агента >, именуемое в дальнейшем «Агент», в лице < должность и ФИО администратора ключей либо иного уполномоченного сотрудника Банка>, действующ(-его)(-ей) на основании <документ>, с другой стороны, в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY» составили настоящий Акт приема - передачи о следующем:

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

Идентификатор Владельца сертификата CN= , OU= , O= , L= , C=

Номер Сертификата

Алгоритм подписи

Заверен

Годен с

Годен до

Алгоритм Ключа проверки электронной подписи

Ключ проверки электронной подписи

Алгоритм отпечатка

Отпечаток

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

От Агента

От Клиента

_____/_____
(Подпись)

_____/_____
(Подпись)

(Дата подписи) М.П.

(Дата подписи)
М.П. (если применимо)

