ДОГОВОР № _____

НА ОБСЛУЖИВАНИЕ КЛИЕНТОВ В СИСТЕМЕ “ИНТЕРНЕТ БАНК-КЛИЕНТ”

г. Москва “____”_____20__ года

ЦМРБанк (общество с ограниченной ответственностью), именуемый в дальнейшем **“БАНК”**, в лице _____, действующего на основании доверенности №_____ от _____ года, с одной стороны, и

заполняется организацией

_____,
(наименование и организационно-правовая форма юридического лица)

именуемое в дальнейшем “**Клиент**”, в лице _____
(должность, фамилия, имя, отчество)

действующего на основании _____,
(Устава или доверенности №, дата)

заполняется индивидуальным предпринимателем

Индивидуальный предприниматель _____,
(фамилия, имя, отчество)

именуемый(ая) в дальнейшем “**Клиент**”, действующий(ая) на основании _____,
(свидетельство №, дата, каким органом выдано)

с другой стороны, в дальнейшем совместно именуемые «Стороны», заключили настоящий договор (далее - **“Договор”**) о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. БАНК и Клиент договариваются об обмене распоряжениями, документами и информацией в электронной форме, подписанными усиленной неквалифицированной электронной подписью (далее – электронная подпись или ЭП), в соответствии с “Регламентом обслуживания с применением Системы “Интернет Банк-Клиент”, далее – “Регламент” (Приложение №2 к настоящему Договору) и «Порядком обмена между БАНКом и Клиентом в электронном виде документами и информацией, связанными с проведением валютных операций», далее – «Порядок» (Приложение №6 к настоящему Договору)».

1.2. Настоящий Договор является неотъемлемой частью заключенного Сторонами Договора[1] **на расчетное и кассовое обслуживание юридических лиц и индивидуальных предпринимателей №** _____ от “___”_____ _____ г., а также договоров, на основании которых открыты счета, указанные в поданной Клиентом в БАНК Заявке на подключение к Системе “Интернет Банк-Клиент”, оформленной по установленной БАНКом форме и являющейся неотъемлемой частью настоящего Договора (Приложение №7) (далее по тексту настоящего Договора именуемой – «Заявление»).

1.3. Стороны признают, что используемые во взаимоотношениях Сторон распоряжения, документы и информация, заверенные электронной подписью, подготовленные и переданные одной Стороной другой Стороне с помощью программного обеспечения Системы “Интернет Банк-Клиент”, равнозначны документам на бумажном носителе и имеют юридическую силу наравне с документами, подписанными уполномоченными представителями Сторон и скрепленными печатью.

1.4. Стороны доверяют используемому программному обеспечению Системы “Интернет Банк-Клиент”.

1.5. Настоящий Договор регулирует отношения Сторон по обмену распоряжениями, документами и информацией, заверенными электронной подписью, подготовленными и переданными одной Стороной другой Стороне с помощью программного обеспечения Системы “Интернет Банк-Клиент”» (в том числе Мобильное приложение «ЦМР Бизнес»), в отношении счетов (далее счет или счета) и операций по счетам, открытым на основании договора, указанного в п. 1.2 настоящего Договора, а также счетов и операций по счетам, указанным в поданном Клиентом в БАНК Заявлении на подключение к Системе "Интернет Банк-Клиент".

В сферу действия настоящего Договора также входят регламентированные в Порядке отношения Сторон по обмену документами и информацией, предусмотренными законодательством о валютном регулировании и валютном контроле.

[1] Указать наименование договора (например, договор Банковского счета и т.п.)

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. БАНК обязуется:
2.1.1. Принимать к проверке и исполнению полученные по Системе “Интернет Банк-Клиент” электронные документы (далее – ЭД), оформленные и заверенные в соответствии с Регламентом (Приложение №2).
2.1.2. Предоставлять Клиенту документы и информацию в соответствии с Приложением №3 к настоящему Договору.
2.1.3. Консультировать персонал Клиента по вопросам обслуживания в Системе “Интернет Банк-Клиент”.
2.1.4. Обеспечивать защиту от несанкционированного доступа и сохранять конфиденциальность информации по счетам Клиента.
2.1.5. Сообщать Клиенту об обнаружении попытки несанкционированного доступа к Системе “Интернет Банк-Клиент”, если это затрагивало операции Клиента, в течение суток с момента обнаружения факта.
2.1.6. Предоставлять Клиенту возможность использования дополнительных услуг в рамках Системы «Интернет Банк-Клиент».
2.1.7. Предоставлять Клиенту доступ к Системе «Интернет Банк-Клиент» только при использовании Клиентом средств и способов защиты передаваемой информации, указанных в Заявлении/Заявлениях.
2.1.8. Информировать клиента о совершении каждой операции с использованием ЭД. Информирование Клиента в Системе «Интернет Банк-Клиент» осуществляется путем изменения статуса обработки ЭД в Системе «Интернет Банк-Клиент» (доставлен/у операциониста/исполнен), а также отражением исполненного ЭД в выписке по счету (счетам).
2.1.9. Предоставлять по запросам другой Стороны подтверждения по ЭД, а также надлежащим образом оформленные бумажные копии ЭД.

2.2. БАНК имеет право:
2.2.1. Изменять Тарифы БАНКа на обслуживание в Системе “Интернет Банк-Клиент” с предварительным уведомлением Клиента за 3 (Три) календарных дня путем размещения информации на стендах в БАНК, и/или на сайте БАНК в сети Интернет, и/или информационным сообщением по Системе “Интернет Банк-Клиент”.
2.2.2. Списывать без дополнительного распоряжения Клиента (на условиях заранее данного акцепта) со счетов Клиента сумму комиссионного вознаграждения за осуществление расчетов с применением Системы “Интернет Банк-Клиент” в соответствии с Тарифами БАНКа.
Настоящим Клиент предоставляет БАНКу право списывать без дополнительного распоряжения Клиента (на условиях заранее данного акцепта) со счета, а также с других счетов Клиента, открытых в БАНКе и подключенных к Системе «Интернет Банк-Клиент», при недостаточности денежных средств на счете, денежные средства на оплату комиссии БАНКа в соответствии с действующими Тарифами в день совершения операции или иной срок, установленный Тарифами БАНКа.
2.2.3. В случае недостаточности денежных средств на счете клиента, а также других счетах, открытых в БАНКе и подключенных к Системе «Интернет Банк-Клиент», для оплаты комиссионного вознаграждения за обслуживание с применением Системы “Интернет Банк-Клиент” в соответствии с Тарифами БАНКа, по истечении 7 (семи) календарных дней с момента возникновения задолженности Клиента прекратить предоставление соответствующей услуги Клиенту.
2.2.4. Не принимать к исполнению от Клиента ЭД, оформленные с нарушением Регламента, с уведомлением Клиента не позднее рабочего дня, следующего за днем получения ЭД, путем указания причин отказа в приеме на обработку ЭД в строке статуса в соответствующем модуле, загруженном с сайта https://cmrbank.ru/.
Отказывать в приеме и оформлении документов, связанных с проведением валютных операций, по основаниям и в сроки, предусмотренные нормативными актами Банка России, с указанием причин отказа.
2.2.5. Не осуществлять операции по счету Клиента в случае недостатка средств на счете, с уведомлением Клиента не позднее рабочего дня, следующего за днем получения распоряжения.
2.2.6. В случае необходимости затребовать от Клиента предоставления распоряжения на бумажных носителях, оформленных в соответствии с требованиями Банка России, и не производить платеж до предоставления данного документа, о чем БАНК обязан сообщить Клиенту в однодневный срок со дня получения распоряжения в электронной форме.
2.2.7. Отказать Клиенту в приёме от него ЭД, о чем БАНК обязан сообщить Клиенту в однодневный срок со дня получения документа в электронной форме с указанием причины отказа. В этом случае ЭД Клиента могут приниматься БАНКом в виде документов, оформленных на бумажном носителе надлежащим образом.

2.3. Клиент обязуется:
2.3.1. Соблюдать требования Регламента (Приложение №2) и Порядка (Приложение №6).
2.3.2. Соблюдать конфиденциальность информации, касающейся Системы “Интернет Банк-Клиент”. В случае обнаружения несанкционированного доступа к Системе в течение дня с момента обнаружения сообщить об этом БАНКу.
2.3.3. Обеспечить безопасность и целостность среды исполнения на своем компьютере или мобильном устройстве (отсутствие вредоносного программного обеспечения и программ-закладок).
2.3.4. Соблюдать конфиденциальность информации, касающейся ключей и паролей, используемых в Системе “Интернет Банк-Клиент”.

2.3.5. Контролировать соответствие суммы платежа и остатка на начало операционного дня на своем счете в БАНКе, получать уведомления БАНК о совершенных операциях с использованием ЭД и осуществлять платежи только в пределах этого остатка за исключением случаев предоставления БАНКом овердрафта по счету клиента, условия которого оговариваются отдельным договором.
2.3.6. В случае компрометации ключа ЭП незамедлительно обращаться в БАНК для принятия необходимых мер (в том числе блокировки работы Клиента в Системе “Интернет Банк-Клиент”).
2.3.7. По требованию БАНКа в соответствии с п. 2.2.6 настоящего Договора предоставить Банку ЭД, оформленные на бумажном носителе в соответствии с требованиями Банка России.
2.3.8. Самостоятельно отслеживать уведомления БАНКа о процессе прохождения ЭД.

2.4. Клиент имеет право:
2.4.1. Получать из БАНКа справочную информацию в соответствии с Приложением №3 к настоящему Договору.
2.4.2. Отзывать распоряжения, переданные в БАНК, посредством передачи сообщения по Системе “Интернет Банк-Клиент” в форме запроса свободного формата в соответствии с Приложением №3 к настоящему Договору, содержащего реквизиты отзываемого распоряжения и причины отзыва, подписанного электронными подписями уполномоченных лиц, указанных в карточке образцов подписей.
Отзыв распоряжений может быть осуществлён только до наступления безотзывности перевода денежных средств.
2.4.3. Направлять в БАНК распоряжения, документы и информацию по Системе “Интернет Банк-Клиент” в соответствии с настоящим Договором.

3. ОТВЕТСТВЕННОСТЬ СТОРОН

3.1. Стороны несут ответственность за достоверность информации, предоставляемой друг другу.
3.2. За неисполнение или ненадлежащее исполнение обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.
3.3. БАНК не несет ответственности за неисполнение или ненадлежащее исполнение распоряжений Клиента, произошедшее из-за нарушения Клиентом Регламента (Приложение №2).
3.4. БАНК возмещает Клиенту все убытки, произошедшие из-за нарушения системы защиты информации по вине БАНКа, в соответствии с действующим законодательством Российской Федерации.
3.5. БАНК не несет ответственности за отказ в приеме и оформлении документов, связанных с проведением валютных операций, произошедший из-за несоблюдения Клиентом Порядка (Приложение №6).

4. ОСОБЫЕ УСЛОВИЯ

4.1. Инициатором сеансов связи с БАНКом всегда является Клиент. Любая просрочка в выполнении БАНКом своих обязательств, которая произошла из-за отсутствия инициативы Клиента в установлении сеанса связи с БАНКом, не влечет за собой ответственности БАНКа.
4.2. Клиент при подписании ЭД ЭП применяет свои ключи электронной подписи, а БАНК при проверке ЭП ЭД - ключи проверки электронной подписи Клиента, являющиеся действующими на момент подписания и передачи документа на обработку соответственно.
Проверка поступающих от БАНКа ЭД осуществляется Клиентом в аналогичном порядке, указанном в настоящем пункте.
Ключи электронной подписи (ключи электронной подписи и соответствующий ему ключ проверки электронной подписи) подписывающей Стороны становятся действующими только после завершения процедур регистрации ключей проверки электронной подписи и ввода в действие ключей электронной подписи. Ключи являются действующими на момент подписания, если они зарегистрированы, не отозваны подписывающей Стороной и срок действия их не окончен.
4.3. При регистрации нового ключа проверки ЭП, регистрируемый ключ проверки ЭП заверяется в распечатанном виде на бумажном носителе, т.е. распечатывается на бумаге в виде Сертификата ключа проверки подписи (Приложение №4 к настоящему Договору) с контрольной записью с указанием даты его регистрации и Стороны, которой принадлежит этот ключ проверки, и заверяется подписями уполномоченных лиц и печатью организации.
Для действующих клиентов возможна регистрация новых ключей без визита в банк, в том числе путем заполнения печатной формы Заявления на выпуск сертификата ключа проверки ЭП (Приложение №12 к настоящему Договору). Порядок смены ключа проверки ЭП и регистрируемого ключа проверки ЭП без визита в БАНК указан в разделе 4 Регламента.
4.4. Смена ключей может быть произведена в любой момент по желанию Стороны, которой принадлежат ключи. Клиент обязан произвести смену принадлежащих ему ключей по требованию БАНКа.
4.5. Все процедуры генерации, обмена, регистрации, перерегистрации, ввода в действие и завершение действия ключей ЭП производятся в соответствии с порядком, предусмотренным в Регламенте.
4.6. Обязательства Сторон по электронным документам, вытекающие из настоящего Договора, возникают после даты подписания Сертификата ключа проверки подписи в Системе “Интернет Банк-Клиент” (Приложение №4 к

настоящему Договору) и регистрации Клиента в Системе “Интернет Банк-Клиент”, а при смене Сертификата ключа проверки подписи без визита в БАНК - в порядке, указанном в разделе 4 Регламента.
4.7. Стороны признают и руководствуются всеми терминами, понятиями, определениями и сокращениями, изложенными в Приложении №1 к настоящему Договору, и используемыми в настоящем Договоре и его Приложениях.
4.8. Сведения, содержащиеся в документах, переданных Сторонами друг другу по Системе “Интернет Банк-Клиент”, персональные электронные адреса, идентификационные параметры, регистрационные номера, пароли и ключи обеих Сторон, используемые для разграничения доступа, передачи и защиты передаваемой информации, а также материалы работы согласительной экспертной комиссии по разбору Споров являются конфиденциальными сведениями. Конфиденциальные сведения не подлежат разглашению третьим лицам ни при каких обстоятельствах, кроме установленного законом порядка.
4.9. Для использования ключей облачной подписи в WEB, задействуется функционал входа в Личный Кабинет с использованием логина и пароля с подтверждением одноразовым кодом, поступающим через СМС или Мобильное приложение (если подключено).

5. РАЗРЕШЕНИЕ СПОРОВ

5.1. Все разногласия, споры и конфликтные ситуации, (далее – “Споры”) возникающие между Сторонами вследствие выполнения настоящего Договора, разрешаются с учетом взаимных интересов путем переговоров в порядке, установленным настоящим Договором, его Дополнениями и Приложениями.
5.2. В случае возникновения Споров между Клиентом и БАНКом по предмету настоящего Договора совместным решением обеих Сторон создается согласительная экспертная комиссия из равного количества представителей от каждой Стороны.
5.3. При рассмотрении Споров, связанных с подлинностью электронных документов, комиссия в своей работе руководствуется "Положением по разбору конфликтных ситуаций, связанных с подлинностью электронных документов" (Приложение №5 к настоящему Договору). В ходе рассмотрения комиссией Спора о подлинности (наличии или отсутствии) документа, исполненного с помощью Системы “Интернет Банк-Клиент” или подписанного электронной подписью, каждая Сторона обязана доказать лишь то, что она своевременно и надлежаще выполнила обязанности, взятые на себя по Договору. Своевременным и надлежащим выполнением Стороной обязанностей признается соблюдение порядка и условий выполнения действий при обмене документами в электронном виде, закрепленных в Договоре и Приложениях к нему. При решении вопросов по всем остальным конфликтам Стороны руководствуются действующим законодательством.
5.4. Свои решения комиссия оформляет в виде актов. Стороны признают решения комиссии, оформленные в соответствии с процедурами, установленными в Приложении №5 к настоящему Договору, обязательными для участников Споров, по которым они вынесены, и обязуются добровольно исполнять решения комиссии по указанным вопросам в установленные в них сроки.
5.5. Сторона, признанная виновной, возмещает убытки другой Стороне в соответствии с действующим законодательством Российской Федерации.
5.6 Уклонение какой-либо Стороны настоящего Договора от участия в создании или работе согласительной экспертной комиссии может привести к невозможности ее создания и работы, но не может привести к невозможности урегулирования Спора в судебном порядке. В случае недостижения соглашения Сторон, отсутствия согласия по Спорам и добровольного исполнения решения комиссии, Споры по настоящему Договору рассматриваются в соответствии с действующим законодательством Российской Федерации.

6. СРОК ДЕЙСТВИЯ ДОГОВОРА И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ

6.1. Договор вступает в силу с момента его подписания обеими Сторонами и действует в течение одного календарного года. Если ни одна из Сторон не заявит о своем желании расторгнуть Договор не позднее, чем за один месяц до окончания срока его действия, Договор автоматически продлевается на каждый последующий календарный год.
6.2. Стороны вправе расторгнуть настоящий Договор в одностороннем порядке. Сторона, прекращающая в одностороннем порядке договорные отношения, обязана письменно уведомить об этом другую Сторону не менее, чем за один месяц до его расторжения, с обязательным исполнением всех обязательств, предусмотренных настоящим Договором. Кроме того, Договор расторгается в случаях, предусмотренных действующим законодательством Российской Федерации, и при расторжении Договора, указанного в п.1.2. настоящего Договора.
6.3. При расторжении настоящего Договора Клиент обязуется обеспечить сохранность не действующих (исключенных Банком из каталога действующих ключей в соответствии с Регламентом) принадлежащих ему ключей электронной подписи, относящиеся к настоящему Договору, и не передавать их третьим лицам. Все другие конфиденциальные сведения хранятся и уничтожаются Сторонами в соответствии с порядком и сроками хранения и уничтожения финансовых документов.
6.4. Стороны согласны с тем, что настоящий Договор в части конфиденциальности паролей и ключей действителен в течение одного календарного года после расторжения настоящего Договора.
6.5. Настоящий Договор может быть изменен или дополнен письменным соглашением Сторон.

6.6. Стороны не несут ответственности по настоящему Договору за ущерб, возникший вследствие действия обстоятельств непреодолимой силы (стихийные бедствия, технические сбои, а также иные обстоятельства), при работе через публичную сеть Интернет, происшедшие по независящим от Сторон причинам, существенно влияющим на функционирование Системы и препятствующим исполнению Сторонами обязательств по настоящему Договору.

7. ПРОЧИЕ УСЛОВИЯ

7.1. Настоящий Договор составлен в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному экземпляру для каждой Стороны.
7.2. В Договор включены следующие Приложения, являющиеся его неотъемлемой частью:
Приложение №1 - Термины, их понятия, определения и сокращения, используемые в настоящем Договоре.
Приложение №2 - Регламент обслуживания с применением Системы “Интернет Банк-Клиент” ЦМРБанк (ООО).
Приложение №3 - Перечень электронных документов, пересылаемых по Системе “Интернет Банк-Клиент”, в соответствии с предоставляемыми Клиенту услугами.
Приложение №4 - Сертификат ключа проверки подписи в Системе “Интернет Банк-Клиент” ЦМРБанк (ООО).
Приложение №5 - Положение по разбору конфликтных ситуаций, связанных с подлинностью электронных документов.
Приложение №6 – Порядок обмена между БАНКом и Клиентом в электронном виде документами и информацией, связанными с проведением валютных операций.
Приложение №7 – Заявка на подключение к Системе "Интернет Банк-Клиент".
Приложение №8 – Мобильное приложение «ЦМР Бизнес» (Приложение №1 к Дополнительному Соглашению)
Приложение №9 – Заявка на подключение/отключение к Мобильному приложению «ЦМР Бизнес» (Приложение №2 к Дополнительному Соглашению).
Приложение №10 – Рекомендации по обеспечению информационной безопасности при использовании Мобильного приложения (Приложение №3 к Дополнительному Соглашению).
Приложение №11 – Политика конфиденциальности при использовании Мобильного приложения (Приложение №4 к Дополнительному Соглашению).
Приложение №12 - Заявления на выпуск сертификата ключа проверки ЭП
7.3. Во всем остальном, что прямо не предусмотрено настоящим Договором, Стороны руководствуются Договором **на расчетное и кассовое обслуживание юридических лиц и индивидуальных предпринимателей** № _____ от "___"_____ _____ года, договорами, на основании которых открыты счета, указанные в Заявлении, и действующим законодательством Российской Федерации.

8. АДРЕСА И ПЛАТЕЖНЫЕ РЕКВИЗИТЫ СТОРОН

БАНК:
ЦМРБанк (общество с ограниченной ответственностью),
Юридический адрес: 127055, г. Москва, ул. Палиха, д.10, стр.7
Фактический адрес: 127055, г. Москва, ул. Палиха, д.10, стр.7

Тел. +7 (495) 980-8044, 8 (800) 250-09-22.
ОГРН 1157700005759, ИНН 7750056670, КПП 770701001, ОКПО 45000256,
БИК 044525059, корреспондентский счет № 30101810345250000059 в ГУ Банка России по Центральному федеральному округу

Клиент:
Адрес:
Телефон:
ОГРН ИНН КПП ОКПО
Банковские реквизиты:

БАНК: **КЛИЕНТ:**

_____ _____
м.п. м.п.

Приложение №1
к Договору на обслуживание
клиентов в Системе "Интернет Банк-Клиент"
№_____ от "__" _____ 20_г.

ТЕРМИНЫ, ИХ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ДОГОВОРЕ

Термины их понятия и определения и сокращения для целей настоящего Договора следует понимать и трактовать следующим образом:

Система "Интернет Банк-Клиент" - автоматизированная организационно-техническая система обеспечения электронного документооборота и безбумажных расчетов между БАНКом и его Клиентами, обеспечивающая подготовку, защиту и обработку документов в электронном виде с использованием электронно-вычислительных средств обработки информации и публичной сети Интернет, а также разбор конфликтных ситуаций.

Документ в электронной форме (электронный документ - ЭД) – документ, представленный в электронной форме в виде файла или записи в базе данных, заверенный электронной подписью, подготовленный с помощью программного обеспечения Системы "Интернет Банк-Клиент" (список электронных документов представлен в Приложении №3).

Защита информации от несанкционированного доступа - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования информации, ее блокирования и т.п.

Электронная подпись (ЭП) – данные, добавляемые к блоку данных и полученные в результате его криптографического преобразования, которые позволяют принимающей Стороне удостовериться в целостности блока данных и подлинности источника данных, а также обеспечить защиту от подлога с принимающей Стороны. Средства ЭП обеспечивают формирование подписи ЭД при его передаче на обработку, а также проверку наличия, аутентификации и не искаженности подписи при обработке документов. Электронная подпись однозначно увязывает в одно целое содержание документа и ключ электронной подписи подписывающего и делает невозможным изменение документа без нарушения подлинности данной подписи.

Подлинность ЭД означает, что данный документ (экземпляр документа) создан в Системе "Интернет Банк-Клиент" без отступлений от принятой технологии. Электронный документ считается подлинным, если он был, с одной стороны, должным образом оформлен, заверен (подписан) ЭП и передан на обработку, а с другой, был принят к исполнению. Свидетельством того, что ЭД принят к исполнению, является уведомление "принят к исполнению" в строке статуса в соответствующем модуле, загруженном с сайта https://cmrbank.ru

Целостность ЭД означает, что после его создания и заверения подписью в его содержание не вносилось никаких изменений.

Авторство ЭД - принадлежность ЭП конкретному физическому лицу - участнику электронного документооборота в Системе "Интернет Банк-Клиент".

Уполномоченные службы БАНКа – подразделения БАНКа, осуществляющие обслуживание системы "Интернет Банк-Клиент".

КЛЮЧИ:

Ключ электронной подписи - ключ, изготавливаемый абонентом Системы "Интернет Банк-Клиент" и предназначенный для формирования им ЭП ЭД. Ключ ЭП хранится в цифровом виде, на специализированном носителе информации, именуемом в дальнейшем "ключевой элемент" или "носитель электронного ключа".

Ключевой элемент (Носитель электронного ключа) – специализированное программно-аппаратное устройство (USB-токен), подключаемое к компьютерному устройству Клиента через интерфейс USB, с интегрированной операционной системой со встроенным средством криптографической защиты информации (СКЗИ), сертифицированным в соответствии с законодательством РФ и разрешенным к применению для реализации функций формирования и проверки электронной подписи и шифрования информации.

Ключ проверки электронной подписи - ключ, автоматически формируемый программными средствами Системы "Интернет Банк-Клиент" при изготовлении ключа электронной подписи и однозначно зависящий

(производный) от него. Ключ проверки предназначен для проверки ЭП ЭД, сформированной данным участником системы “Интернет Банк-Клиент” при подписании ЭД. Ключ проверки считается принадлежащим абоненту, если он был зарегистрирован в установленном порядке.

Облачная электронная подпись (облачная ЭП) - вычислительная система, предоставляющая через сеть доступ к возможностям создания, проверки ЭП и интеграции этих функций в бизнес-процессы других систем.

Мобильное приложение Системы “Интернет Банк-Клиент” (далее Мобильное приложение) – канал доступа к Системе “Интернет Банк-Клиент” с использованием специализированного программного обеспечения (приложения), установленного на мобильное устройство Клиента.

Мобильное устройство – переносное мобильное устройство Клиента, такое как смартфон, на базе операционной системы Android, которые имеют технические характеристики, позволяющие использовать функционал Мобильного приложения.

Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- утрата ключевых элементов;
- утрата ключевых элементов с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП;
- несанкционированное копирование или подозрение на копирование информации с Носителя электронного ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с носителями электронных ключей, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- возникновение подозрений на установку вредоносного программного обеспечения на компьютерное устройство с которого выполняется доступ к Системе “Интернет Банк-Клиент”, в том числе с использование облачной ЭП;
- утрата Мобильного устройства или возникновение подозрений на доступ третьих лиц к Мобильному устройству или Мобильному приложению.

Сертификат ключа проверки подписи – электронный документ или документ на бумажном носителе, подтверждающий принадлежность ключа проверки участнику Системы «Интернет Банк-Клиент», заверенный ЭП либо собственноручными подписями владельца соответствующего ключа электронной подписи, уполномоченного лица и печатью организации пользователя Системы “Интернет Банк-Клиент”.

Проверка ЭП ЭД – проверка соотношения, связывающего ЭП под этим ЭД и ключ проверки подписавшего абонента. Если рассматриваемое соотношение оказывается выполненным, то ЭП признается правильной, а сам ЭД – подлинным, в противном случае ЭД считается измененным, а ЭП под ним недействительной.

Приложение №2
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

РЕГЛАМЕНТ ОБСЛУЖИВАНИЯ С ПРИМЕНЕНИЕМ СИСТЕМЫ “ИНТЕРНЕТ БАНК-КЛИЕНТ” ЦМРБанк (ООО)

1. ВВЕДЕНИЕ

Автоматизированная система электронного документооборота (далее Система “Интернет Банк-Клиент”) предназначена для подготовки, учета и предварительной обработки распоряжений Клиентов, а также других ЭД Клиента БАНКа. Она построена на основе технологии всемирной сети интернет, обеспечивает конфиденциальность, надежность и достоверность информации, установление подлинности отправителя, проверку целостности и авторства документа. Также реализована возможность доказательного разрешения споров на основе применения системы защиты, состоящей из специальных программных и технических средств, организационных мер и договорно-правовых норм.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Электронные документы, применяемые в Системе “Интернет Банк-Клиент”, юридически эквивалентны документам, предоставляемым на бумажном носителе, используемым в соответствии с нормативными актами Банка России и настоящим Договором и являются основанием для осуществления операции по счету (счетам) Клиента.
Стороны признают, что используемая по настоящему Договору система телекоммуникации, обработки и хранения информации является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а система защиты информации, обеспечивающая разграничение доступа, шифрование, контроль целостности и электронную подпись, является достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, и для разрешения спорных ситуаций.
Электронный документ (ЭД) порождает обязательства Сторон по настоящему Договору, если он инициирующей Стороной должным образом оформлен, заверен электронной подписью и передан на обработку, а принимающей Стороной принят к исполнению. Свидетельством того, что ЭД принят к исполнению, является уведомление “принят к исполнению” в строке статуса в соответствующем модуле, загруженном с сайта https://cmrbank.ru.
Готовность Сторон к работе по Системе “Интернет Банк-Клиент” оформляется подписанием Сертификата ключа проверки подписи в системе “Интернет Банк-Клиент” (Приложение №4 к Договору) и регистрации Клиента в Системе “Интернет Банк-Клиент”.

2.1 В рамках настоящего Регламента БАНК осуществляет следующие функции:
2.1.1. Прием от Клиента по электронным каналам связи должным образом оформленных электронных документов с контролем их целостности и авторства.
2.1.2. Прием ЭД только с верной электронной подписью уполномоченных лиц (ЭП), регистрационный идентификационный номер и ключ проверки которых соответствует данным, указанным в Сертификате ключа проверки подписи в Системе “Интернет Банк-Клиент” (Приложение №4 к Договору) и в Заявлении на выпуск сертификата ключа проверки ЭП (Приложение №12 к Договору).
2.1.3. Обработку и исполнение полученных ЭД Клиента в строгом соответствии с установленными нормами, техническими требованиями, стандартами, инструкциями Банка России и БАНКа.
2.1.4. Предоставляет Клиенту информацию о результатах проверки и обработки (или отказе в приеме на обработку с указанием причин) принятого ЭД Клиента.
2.1.5. По результатам обработки и исполнения ЭД Клиента, а также по мере совершения иных операций по счету, в течение следующего дня после совершения операции, подготавливает и предоставляет Клиенту, в ответ на его запрос, выписки по счету с указанием основных реквизитов платежного документа, на основании которого совершена операция по счету.
2.1.6. Своевременно информирует Клиента об изменениях порядка осуществления обработки ЭД и другой информации по Системе «Интернет Банк-Клиент». Оказывает консультационные услуги Клиенту по вопросам, необходимым для правильной эксплуатации Системы «Интернет Банк-Клиент» Клиентом, как-то: функционирование Системы «Интернет Банк-Клиент», использования средств защиты и технологии обработки информации.
2.1.7. Осуществляет необходимую модернизацию программного обеспечения Системы «Интернет Банк-Клиент» и информирует Клиента о предстоящей модернизации за 10 (Десять) календарных дней, размещая

информацию на сайте БАНКа.
2.1.8. Сообщает Клиенту о непредвиденных сбоях в работе Системы «Интернет Банк-Клиент» для принятия им мер по своевременной доставке распоряжения на бумажном носителе в БАНК. Доставка распоряжения, документов на бумажном носителе осуществляется Клиентом в течении действующего операционного дня БАНКа.

2.2. В соответствии с настоящим Регламентом Клиент обязуется
2.2.1. Осуществлять ввод документов (и осуществлять контроль введенной информации) в электронном виде, соблюдая порядок подготовки документов, обеспечивая заполнение форм в соответствии с требованиями БАНКа.
2.2.2. Осуществлять в течение любого рабочего дня не менее одного сеанса связи с БАНКом для получения возможных экстренных (технических) сообщений от БАНКа, либо другой актуальной информации.
2.2.3. Выполнять требования по оформлению и защите передаваемой информации в виде ЭД, защите ключей ЭП, паролей доступа и другой информации, передаваемой и получаемой по Системе «Интернет Банк-Клиент».
2.2.4. Соблюдать порядок осуществления приема и передачи ЭД и обеспечивать передачу только надлежащим образом оформленных документов.

2.3. Стороны обязуются соблюдать следующие условия
2.3.1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования Системы «Интернет Банк-Клиент».
2.3.2. Поддерживать системное время компьютерного устройства своего абонентского пункта по местному времени с точностью до пяти минут. При обработке документов, полученных по Системе «Интернет Банк-Клиент», определяющим временем является текущее время по системным часам аппаратных средств БАНКа.
2.3.3. Не осуществлять операцию по ЭД, заверенному ЭП, если программа проверки, используя действующий ключ проверки подписывающей Стороны, не подтвердила подлинность ЭП подписывающей Стороны под ЭД.
2.3.4. При осуществлении операций на основании полученных по Системе «Интернет Банк-Клиент» ЭД руководствоваться требованиями законодательства Российской Федерации и Договоров, заключенных между БАНКом и Клиентом.
2.3.5. Обеспечивать целостность и сохранность программных средств, ЭД, защиту ключей ЭП, паролей доступа и другой информации, передаваемой и получаемой по Системе «Интернет Банк-Клиент».
2.3.6. Вести архивы документов на магнитных и бумажных носителях, хранить их в соответствии с порядком и сроками, установленными для хранения данного вида документов.
2.3.7. За собственный счет поддерживать в рабочем состоянии и при необходимости самостоятельно модернизировать свои помещения и технические средства обеспечения работоспособности вычислительной техники, средств связи, автоматизированного рабочего места, с которого осуществляется работа с Системой «Интернет Банк-Клиент».

3. УСЛОВИЯ И ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

3.1. Общие положения
3.1.1. Программное обеспечение БАНКа настроено на взаимодействие с системой программного обеспечения “Интернет Банк-Клиент”, разработанной АО “БИФИТ”, и предполагает использование этой Системы «Интернет Банк-Клиент» Клиентом.
3.1.2. БАНК и Клиент взаимно признают достоверность ЭП, созданной программной Системой “Интернет Банк-Клиент”, разработанной АО “БИФИТ”, на ЭД, передаваемых согласно условиям Договора.
3.1.3. После подписания Договора Стороны проводят техническую и организационную подготовку, регистрацию ключей проверки ЭП.
3.1.4. Документы, переданные по Системе “Интернет Банк-Клиент”, приобретают юридическую силу после получения уполномоченными службами БАНКа должным образом оформленного и подписанного Сертификата ключа проверки подписи в Системе “Интернет Банк-Клиент” (Приложение №4 к Договору) и регистрации Клиента в Системе “Интернет Банк-Клиент”.
3.1.5. ЭД представляют собой электронные бланки документов, заполняемые Клиентом на ресурсе БАНКа https://ibank.cmrbank.ru в соответствии с требованиями БАНКа. На экран компьютерного устройства Клиента выводится электронный бланк, который заполняется согласно наименованиям полей и правилам, принятым в БАНКе. Некоторые поля заполняются автоматически в соответствии со встроенными справочниками реквизитов. Заполнение документов возможно только после установления защищенного (с использованием алгоритмов шифрования и обеспечения целостности) соединения между Клиентом и БАНКом.
3.1.6. Заполняемые в Системе «Интернет Банк-Клиент» документы проходят предварительную автоматическую проверку (на датировку документа, на присутствие обязательной информации в полях документа, на соответствие вводимых данных - реквизитам, записанным во встроенном справочнике и иное в соответствии с принятой технологией).
3.1.7. На этапе обработки документов в БАНКе осуществляется автоматический контроль (на соответствие электронной подписи содержимому документа, на правильность указанного номера счета Клиента, на соответствие реквизитов БАНКа и РКЦ получателя установленным Банком России и иное в соответствии с

принятой технологией). В случае выявления несоответствий в ходе проверки документа, операции по документу не проводятся, а Клиент получает информацию с указанием причин отказа в приеме на обработку ЭД в строке статуса в соответствующем модуле, загруженном с сайта https://ibank.cmrbank.ru.
3.1.8. После заполнения электронной формы платежного или иного документа Клиентом осуществляется подписание документа. Подробности порядка работы с электронными документами описаны во встроенной в Систему «Интернет Банк-Клиент» документации.
3.1.9. Основанием для отказа БАНКом от исполнения ЭД служат:
- отрицательный результат проверки электронной подписи;
- недостаток денежных средств для проведения операций на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- несоответствие даты документа требованиям действующего законодательства Российской Федерации;
- неверно указанные реквизиты отправителя или получателя платежа;
- несоответствие ЭД требованиям Банка России и БАНКа.
3.1.10. Активной стороной при установлении связи является Клиент.

3.2. Сроки обработки платежей
3.2.1. Работа Системы «Интернет Банк-Клиент» обеспечивается БАНКом в течение времени, установленного БАНКом для обслуживания Клиентов. Информация о времени обслуживания Клиентов и приема расчетных документов доводится до сведения Клиента путем размещения на информационных стендах в офисах БАНКа и на сайте БАНКа по адресу: https://cmrbank.ru

3.3. Аварийный режим работы
3.3.1. При возникновении неисправности технических или программных средств Клиента, или других нештатных ситуаций, Клиент до 14 часов местного времени, того же дня, должен предупредить уполномоченных сотрудников БАНКа, и осуществить действия для доставки в БАНК надлежащим образом оформленных распоряжений и других ЭД на бумажных носителях. Доставка распоряжения, документов на бумажном носителе осуществляется Клиентом в течении действующего операционного дня БАНКа.

4. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. Общие положения
4.1.1. Защита информации в Системе «Интернет Банк-Клиент» является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения и специализированных программных и технических средств и организационных мер (наличие соответствующих администраторов), организации хранения ПО, используемого в Системе «Интернет Банк-Клиент».
4.1.2. Система комплексной защиты информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:
создание ключей шифрования и электронной подписи;
электронную подпись под документами;
шифрование передаваемой информации;
аутентификацию Клиентов и разграничение их прав;
достоверность факта получения документа получателем;
подтверждение авторства и целостность электронных документов;
выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
разбор конфликтных ситуаций.
4.1.3. Для разрешения возможных споров в БАНКе ведутся контрольные архивы ЭД подписанных ЭП, а также архивы ключей проверки электронной подписи. Хранение контрольных архивов ЭД осуществляется в течение пяти лет с момента проведения операции.
4.1.4. При проверке подписи под электронным документом используется соответствующий ключ подписи Клиента, подписавшего электронный документ.

4.2. Порядок генерации ключей ЭП
4.2.1. Клиентам при первичной регистрации или создании нового ключа доступен выбор типа ЭП – ЭП на Носителе электронного ключа или облачная ЭП. При выборе ЭП на Носителе, запустится процедура регистрации, согласно п. 4.2.2 Регламента. При выборе Облачной ЭП, в случае первичной регистрации, создается учетная запись для входа по логину и паролю, ЭП в облачном хранилище.
Действующие клиенты имеют возможность самостоятельно подключить вход по логину и паролю в настройках Личного кабинета, для этого указывается адрес электронной почты в качестве логина и номер телефона, далее, по ссылке, пришедшей на электронную почту для подтверждения регистрации вводится одноразовый пароль, полученный через СМС.
4.2.2. В процессе первичной регистрации Клиент самостоятельно создает ключ ЭП и парный ему ключ проверки ЭП. Ключ ЭП Клиента сохраняется на Носитель электронного ключа Клиента. Ключ проверки ЭП по защищенному соединению передается в БАНК и предварительно регистрируется. Также ключ проверки ЭП распечатывается Клиентом на бумажном носителе в виде Сертификата ключа проверки подписи в Системе

“Интернет Банк-Клиент” (Приложение №4 к Договору), далее подписывается руководителем и главным бухгалтером Клиента, заверяется оттиском печати организации и регистрируется в БАНКе согласно п.4.2.5. данного Регламента. Распечатка Сертификата ключа проверки подписи хранится в БАНКе, а ее электронный аналог находится в каталоге ключей БАНКа и Клиента.
4.2.3. Все ключи ЭП защищаются паролями и данный пароль является конфиденциальной информацией соответствующей Стороны.
4.2.4. Владельцы Сертификатов ключа проверки подписи несут персональную ответственность за обеспечение сохранности ключевой информации и защиту Носителя электронного ключа от несанкционированного доступа.
4.2.5. Все процедуры окончательной регистрации Клиента и проверки ключей проверки ЭП происходят в помещении, на программном обеспечении и оборудовании БАНКа.
4.2.6. При регистрации ключа проверки ЭП Клиента в БАНКе производится сверка ключа проверки ЭП Клиента с ключом проверки, напечатанным в Сертификате ключа проверки подписи, и проверка данных на лиц, на имя которых сформированы ключи, на соответствие с именами, фамилиями, образцами подписей и оттиском печати, указанными в карточке Клиента, хранящейся в БАНКе.
При регистрации ключей без права подписи производится сверка Ф.И.О., подписи и должности Уполномоченных лиц Клиента, указанных в Сертификате, на соответствие данным представителей Клиента, содержащихся в документах, удостоверяющих личность, и документах, подтверждающих наличие соответствующих полномочий представителя Клиента без права электронной подписи (Доверенность).
4.2.7. Ключ активируется только после получения заверенного Клиентом Сертификата ключа проверки подписи и положительных результатах проверки данных, указанных в п.п. 4.2.5.

4.3. Порядок хранения и смены ключей ЭП
4.3.1. Порядок хранения ключей
4.3.1.1. Надежность средств криптозащиты и подлинность передаваемой по каналам связи информации обеспечивается только при условии сохранности от компрометации (утрата, копирование и т.п.) действующих ключей ЭП.
4.3.1.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение своих ключей ЭП, хранящиеся на Носителе электронного ключа. В случае потери, кражи, несанкционированного копирования или любого подозрения о компрометации ключей Клиент обязан немедленно оповестить БАНК, прислав в дальнейшем подтверждение в письменной форме.
4.3.1.3. БАНК и Клиент обеспечивают сохранность ключей. При этом выведенные из употребления ключи проверки ЭП хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.
4.3.2. Порядок смены ключей ЭП
4.3.2.2. Смена ключей производится при:
- Замене карточки Клиента.
- Истечении срока действия ключей.
- Компрометации ключей.
- Заявлении Клиента в письменной форме.

4.3.2.3. Срок действия ключей устанавливается в 365 дней с момента их изготовления.
4.3.2.4. Смена ключей уполномоченных лиц Клиента производится в соответствии с п.4.2.1. данного Регламента.
4.3.2.5 ЭД, подписанный ЭП с использованием новых ключей, принимается БАНКом только после получения Сертификата ключа проверки подписи и проведения регистрации ключей в соответствии п.п. 4.2.5. данного Регламента.
4.3.3. Порядок смены ключей ЭП при истечении срока действия (без визита в БАНК)
4.3.3.1. Смена ключей ЭП без визита в БАНК доступна только уполномоченным лицам Клиента (владельцам действующих ключей ЭП) до окончания срока действия используемых ключей ЭП.
4.3.3.2. Смена ключей ЭП без визита в БАНК, у которых истек срок действия, не возможна.
4.3.3.3. Создание нового ключа ЭП и ключа проверки ЭП в Системе «Интернет Банк-Клиент» происходит в соответствии с п.4.2. данного Регламента за исключением необходимости предоставления в Банк Сертификата ключа проверки ЭП на бумажном носителе.
4.3.3.4. По результатам прохождения всех этапов создания ключа ЭП в Системе «Интернет Банк-Клиент» автоматически создается предзаполненное заявление на выпуск Сертификата ключа проверки ЭП, которое подписывается текущим ключом Клиента. Далее, в автоматическом режиме по защищенному соединению передается в БАНК для проверки и регистрации.
4.3.3.5. После приема, успешной проверки, исполнения заявления и активации ключа ЭП на стороне БАНКа новый ключ ЭП может быть использован Клиентом для работы в Системе «Интернет Банк-Клиент».

4.4. Порядок блокировки ключей ЭП
4.4.1. БАНК блокирует (приостанавливает действие) ключа с момента получения уполномоченными службами БАНКа письменного заявления Клиента о блокировке ключа (содержащего причину блокировки), составленного в произвольной форме, подписанного руководителем и главным бухгалтером Клиента и заверенного оттиском печати организации. В экстренных случаях, блокировка может быть произведена при уведомлении иным способом (по телефону, по электронной почте, факсу и т.п.) с последующим

предоставлением подписанного заявления на бумажном носителе в течение трех рабочих дней. После блокирования ключа, прием и обработка документов, подписанных данным ключом, прекращается.
4.4.2. БАНК может блокировать ключ Клиента самостоятельно, в случае возникновения подозрений в компрометации ключа. В этом случае уполномоченный сотрудник БАНКа немедленно извещает Клиента о принятом решении и о приостановлении обработки ЭД, подписанных этим ключом по телефону или с использованием других средств связи.
4.4.3. Снятие блокировки производится на основании заявления Клиента, подписанного руководителем и главным бухгалтером и заверенном оттиском печатью организации, об устранении причин, приведших к блокированию ключа. В случае блокировки ключа по инициативе БАНКа снятие блокировки с ключа Клиента производится по согласованию с Клиентом и с его письменного разрешения.

4.5. Порядок исключения ключей ЭП
4.5.1. БАНК исключает (блокирует, удаляет) ключ из каталога (базы) действующих ключей проверки, с момента получения уполномоченными службами БАНКа письменного заявления Клиента, составленного в произвольной форме и подписанного руководителем и главным бухгалтером и заверенного оттиском печати организации. Ключ исключается из каталога ключей проверки, прием и обработка ЭД, подписанных данным ключом прекращается.
4.5.2. БАНК и Клиент обеспечивают сохранность исключенных ключей согласно п.п. 4.3.1. данного Регламента. При этом исключенные ключи хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.

4.6. Порядок действий в случае компрометации ключей ЭП:
4.6.1. В случае компрометации или подозрения на компрометацию ключа Клиент должен незамедлительно известить уполномоченных сотрудников БАНКа для блокировки соответствующего ключа, в соответствии с порядком, установленным п.п. 4.4. данного Регламента.
4.6.2. В случае не подтверждения компрометации ключа, БАНК производит снятие блокировки ключа в соответствии с п.п. 4.4.3. данного Регламента.
4.6.3. В случае подтверждения компрометации ключа БАНК исключает скомпрометированный ключ в соответствии с п.п. 4.5. данного Регламента.
4.6.4. ЭД, подписанные скомпрометированным ключом, и ключ проверки ЭП хранятся в соответствии с п.п. 4.3.1.3. данного Регламента.

4.7[2]. Порядок предоставления Клиенту одноразовых паролей для отправки документов в БАНК с использованием Системы «Интернет Банк-Клиент».
4.7.1. По желанию Клиента, для целей дополнительной защиты от несанкционированного проведения платежей БАНК может оказать Клиенту дополнительную услугу по предоставлению одноразовых паролей для отправки документов в БАНК с использованием Системы «Интернет Банк-Клиент».
4.7.2. БАНК предоставляет Клиенту одноразовые пароли:
- посредством SMS-сообщений, направляемых на указанные Клиентом номера мобильных телефонов (не более трех номеров);
4.7.3. Для подключения к услуге Клиент обращается в БАНК и оформляет Заявление по установленной БАНКом форме.
На основании Заявления БАНК подключает Клиента к услуге. Оплата услуги осуществляется в соответствии с действующими в Тарифами БАНК.
4.7.4. В любой момент времени в течение срока действия Договора Клиент на основании Заявления, оформленного по форме БАНКа, может заменить действующие телефонные номера для SMS-информирования (общее количество действующих телефонных номеров для SMS- информирования – не более трех).
Оплата услуги осуществляется в соответствии с действующими Тарифами БАНКа.
4.7.5. Клиент может отказаться от предоставляемой БАНКом услуги дополнительного подтверждения операций в Системе «Интернет Банк-Клиент».
При отказе Клиента от услуги по представлению одноразовых паролей плата за предоставление услуги возврату Клиенту не подлежит.
Отказ Клиента от предоставления услуги осуществляется на основании Заявления Клиента.
4.7.6. В случае подключения услуги, при работе с Системой «Интернет Банк-Клиент» Клиент подтверждает одноразовым паролем, получаемым посредством SMS-сообщения:
- первичный вход в Систему «Интернет Банк-Клиент»;
- совершение расходных операций по счету Клиента (допускается одновременное подтверждение одноразовым паролем отправки нескольких сформированных документов) с использованием Системы «Интернет Банк-Клиент».

[2] Раздел 4.7., выделенный курсивом, включается при наличии в Банке услуги по предоставлению одноразовых паролей для отправки документов в БАНК с использованием Системы «Интернет Банк-Клиент» При отсутствии в Банке указанной услуги, раздел 4.7. необходимо исключить из текста.

4.7.7. БАНК осуществляет контроль аутентичности (подтверждения подлинности) одноразового пароля, формируемого посредством SMS-сообщения. В случае выявления несоответствий в ходе проверки документа, операции по документу не проводятся, а Клиент получает информацию с указанием причин отказа в приеме на обработку ЭД в строке статуса в соответствующем модуле, загруженном с сайта https://cmrbank.ru.
Основанием для отказа БАНКом от исполнения электронного документа служит отрицательный результат проверки аутентичности одноразового пароля.
4.7.8. В случае компрометации номера мобильного телефона (например, в случае утраты мобильного телефона) номер мобильного телефона должен быть заблокирован. Блокирование Клиент должен осуществить по телефону с использованием блокировочного слова – набора символов, введенных Клиентом самостоятельно в процессе предварительной регистрации на сайте БАНКа, предназначенного для голосовой аутентификации (подтверждения подлинности) Клиента во время телефонных переговоров Клиента с БАНКом с целью временно блокировать работу в Системе «Интернет Банк-Клиент». После этого Клиент должен подключить новый номер мобильного телефона. Подключение нового номера мобильного телефона осуществляется в соответствии с требованиями п. 4.7.3 настоящего Регламента.
4.7.9. БАНК не несет ответственности за качество услуг, предоставляемых операторами мобильной связи.

Приложение №3
к Договору на обслуживание
клиентов в Системе "Интернет Банк-Клиент"
№_____ от "__" _____ 20_г.

ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ,
ПЕРЕСЫЛАЕМЫХ ПО СИСТЕМЕ "ИНТЕРНЕТ БАНК-КЛИЕНТ",
В СООТВЕТСТВИИС ПРЕДОСТАВЛЯЕМЫМИ КЛИЕНТУ УСЛУГАМИ

Виды сообщений, которые Клиент передает в БАНК по Системе "Интернет Банк-Клиент":

№пп	***Наименование ЭД***	***Вид сообщения***
1	***2***	***3***
	Документы по счетам Клиента	
1	Платежное поручение в рублях;	Формализованное
2	Заявление на аккредитив;	Формализованное
3	Платежное требование;	Формализованное
4	Инкассовое поручение;	Формализованное
5	Заявление об акцепте / отказе от акцепта;	Формализованное
6	Заявление на получение наличных денежных средств;	Формализованное
7	Реестр переданных на инкассо платежных требований;	Формализованное
8	Заявление на перевод средств в иностранной валюте;	Формализованное
9	Заявление на открытие импортного аккредитива;	Формализованное
10	Распоряжение на покупку иностранной валюты;	Формализованное
11	Поручение на покупку валюты за другую валюту;	Формализованное
12	Поручение на продажу иностранной валюты;	Формализованное
13	Распоряжение на обязательную продажу валюты;	Формализованное
14	Зарплатный реестр;	Формализованное
15	Запросы по вопросам расчетов и другим видам услуг, предоставляемых в БАНК (в соответствии с адресной книгой)	Свободный формат
16	Прочие сообщения и запросы	Свободный формат
	Документы для целей валютного контроля	
17	Паспорт сделки по контракту	Формализованное
18	Паспорт сделки по кредитному договору	Формализованное
19	Справка о валютных операциях	Формализованное
20	Справка о подтверждающих документах	Формализованное
21	Прочие сообщения и запросы	Свободный формат

Виды сообщений, которые Клиент получает по Системе "Интернет Банк-Клиент" из БАНКа:

№пп	***Наименование ЭД***	***Вид сообщения***
1	***2***	***3***
	Документы по счетам Клиента	
1	Выписки по рублевым счетам Клиента, включая остатки по счетам и приложения к выписке;	Формализованное
2	Выписки по валютным счетам Клиента, включая остатки по счетам и приложения к выписке;	Формализованное
3	Оборотно-сальдовая ведомость;	Формализованное
4	Платежное требование, выставленное Клиенту;	Формализованное
5	Прочие сообщения и запросы	Свободный формат

Перечень и формы ЭД могут меняться в связи с изменениями нормативных актов Банка России и с учетом развития системы и услуг, предоставляемых Клиентам БАНКа при использовании Системы **«Интернет Банк-Клиент»**.

Приложение №4
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ПОДПИСИ
В СИСТЕМЕ “ИНТЕРНЕТ БАНК-КЛИЕНТ”
ЦМРБАНК (ООО)

1. Наименование организации _____
2. Юридический адрес _____
3. Местонахождение _____
4. Наименование документа о регистрации, кем и когда выдан _____
_____
5. Тел. _____ 6. Факс _____7. E-mail _____
8. Примечания: _____
9.Сведения о владельце ключа:
Фамилия, имя, отчество _____
Должность _____
Паспорт: сер._____ № _____ выдан _____
дата выдачи "____ "_____ _____ г. код подразделения _____

Личная подпись
владельца ключа

Информация о ключе проверки ЭП:

Идентификатор ключа проверки ЭП: _____ Идентификатор токена:
_____
Наименование криптосредств: _____
Алгоритм: _____
Представление ключа проверки ЭП в шестнадцатеричном виде:
_____
_____
_____
_____
_____
_____
_____

Дата начала действия ключа "___" _____ 20_ г.
Дата окончания действия ключа "___" _____ 20_ г.

Достоверность приведенных данных подтверждаю
Руководитель организации _____ (_____)
ФИО

Главный бухгалтер _____ (_____)
ФИО

Оттиск печати

"___"_____20_ г.

Уполномоченный представитель БАНК _____ (_____)
ФИО

Администратор системы/Уполномоченный контролер БАНК _____ (_____)
ФИО

Оттиск печати БАНК

"___"_____20_ г.

Приложение №5
к Договору на обслуживание
клиентов в Системе "Интернет Банк-Клиент"
№_____ от "__" _____ 20_г.

ПОЛОЖЕНИЕ
ПО РАЗБОРУ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПОДЛИННОСТЬЮ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В данном Положении описан порядок разрешения конфликтных ситуаций между БАНКом и Клиентом, связанных с подлинностью электронных документов, исполненных в Системе "Интернет Банк-Клиент".
Электронный документ считается подлинным, если он был, с одной стороны, надлежащим образом оформлен и подписан, а с другой - проверен и принят.
При наличии сомнений в подлинности ЭД или его содержания Сторона - инициатор спора обязана направить другой Стороне письмо с подробным изложением нарушения, обстоятельств происшедшего и предложением создать согласительную экспертную комиссию.
1.2. В случае согласия с претензией, содержащейся в письме, Сторона, получившая письмо, незамедлительно уведомляет другую Сторону и устраняет нарушения, описанные в письме. Согласительная экспертная комиссия в таком случае не создается.
1.3. *Примечание*: До подачи письменного заявления сторонам рекомендуется проверить, что причиной возникновения Спора не является *нарушение целостности программного обеспечения, целостности среды исполнения на компьютере Клиента,* компрометация ключей ЭП или несанкционированный доступ к ресурсам.

2. РАБОТА СОГЛАСИТЕЛЬНОЙ ЭКСПЕРТНОЙ КОМИССИИ

2.1. Для рассмотрения Споров создается согласительная экспертная комиссия. Данная комиссия создается только по письменному заявлению одной из Сторон. Дата сбора комиссии назначается не позднее 15 (Пятнадцать) календарных дней с момента отправки предложения о ее создании. В состав комиссии входит равное количество представителей обеих Сторон. При необходимости, с согласия обеих Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Состав комиссии должен быть зафиксирован в итоговом документе (Акте), отражающем результаты работы комиссии.
2.2. Экспертная комиссия осуществляет свою работу на территории БАНКа, с использованием компьютерных устройств, программного обеспечения и ключевых элементов.
2.3. Срок работы комиссии – 5 (Пять) рабочих дней. В особо сложных случаях, по обоюдному письменному согласию Сторон, этот срок может быть увеличен, но не более чем до одного месяца.
2.4. Целью работы созданной комиссии является установление подлинности ЭД, исполненного в рамках Договора.
2.5. Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы. Стороны способствуют работе комиссии и не допускают отказа от представления необходимых документов, имеющих отношение к рассматриваемому Спору.
2.6. В ходе рассмотрения комиссией Спора о подлинности (наличии или отсутствии) документа, исполненного с помощью Системы «Интернет Банк-Клиент» и подписанного ЭП, каждая Сторона обязана доказать лишь то, что она своевременно и надлежащим образом выполнила обязательства, взятые на себя по Договору и Приложениям к нему.
2.7. По итогам работы комиссии составляется Акт, в котором в обязательном порядке отражаются:
- установленные обстоятельства;
- действия членов комиссии;
- выводы о подлинности предъявленного электронного документа;
- основания, послужившие для формирования выводов.

Акт подписывается уполномоченными представителями Сторон не позднее 10 (Десяти) календарных дней с момента окончания работы комиссии. В случае, если подписание Акта в этот срок не состоится, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения, а в качестве доказательства в судебном споре представить Акт, составленный в соответствии с настоящим Положением.
2.8. В случае, если предложение о создании комиссии оставлено другой Стороной без ответа (по истечении 15 (Пятнадцати) календарных дней согласно п.2.1. данного Положения), либо Сторона отказывается от участия в комиссии, либо работе комиссии были учинены препятствия, которые не позволили комиссии оформить надлежащий Акт, заинтересованная Сторона составляет Акт в одностороннем порядке с указанием причины составления его в одностороннем порядке. В указанном Акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый электронный документ, произведенный в Системе в соответствии с

Договором, является подлинным, либо формулируется вывод об обратном. Указанный Акт направляется другой Стороне для сведения.

3. РАССМАТРИВАЕМЫЕ СПОРЫ

3.1. Согласительная экспертная комиссия рассматривает споры следующих основных типов, (данный список не является исчерпывающим):
Сторона-получатель ЭД утверждает, что инициирующая Сторона-отправитель должным образом оформила, заверила (подписала) ЭП и передала на обработку документ, а Сторона-отправитель отрицает факт подготовки, заверения (подписания) ЭП и передачи на обработку этого документа. В этом случае Сторона-получатель предъявляет комиссии ключ проверки подписи Стороны-отправителя в электронном виде и файл, содержащий спорный ЭД, подписанный ЭП Стороны-отправителя. На специально выделенном компьютере устанавливается эталонное программное обеспечение для проверки корректности ЭП под документом. С помощью программы проверки ЭП проверяется корректность ЭП файла, содержащего оспариваемый ЭД. В том случае, если корректность ЭП подтверждается программой, виновной признается Сторона-отправитель ЭД, в противном случае виновной признается Сторона-получатель ЭД.

4. ПОРЯДОК ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭП под ЭД

4.1. Последовательность формирования электронной подписи под электронным документом следующая:
4.1.1. Подписываемый электронный документ состоит из набора полей и представляется в виде:

<Наименование поля 1>=<Значение поля 1> <символ перевода строки>

<Наименование поля 2>=<Значение поля 2> <символ перевода строки>

……...
4.1.2. Подписываемый ЭД в виде набора полей, описанного в п.4.1.1, преобразовывается в строку символов, и далее в соответствии с кодировкой UniCode преобразовывается в байтовый массив.
4.1.3. Электронная подпись формируется от указанного в п.4.1.2 байтового массива в соответствии ГОСТ Р34.10-2001.
4.1.4. Публичные параметры P,Q,A и таблица подстановок для вычисления хеш-функции в соответствии с ГОСТ Р34.11-94 при контрольной проверке ЭП для указанного в п.4.1.2 байтового массива представляются в БАНК в шестнадцатиричном виде по запросу согласительной экспертной комиссии.
4.2. Контрольная проверка электронной подписи Клиента под электронным документом, пришедшим в БАНК, осуществляется в АРМе “Операционист”, входящим в комплекс Системы “Интернет-Банк” или при помощи иного Программного обеспечения, применяемого в БАНКе на момент проведения контрольной проверки.
При проверке ЭП Клиента в АРМе “Операционист”, отображается:

- Содержание электронного документа
- Идентификаторы ключей ЭП Клиента, которыми подписан ЭД
- Время формирования ЭП (если документ подписан несколькими ЭП – время формирования каждой ЭП)
- Результаты проверки каждой из ЭП под ЭД

Результат проверок ЭП Клиента под ЭД в АРМе “Операционист” или в ином Программном обеспечении, применяемом в БАНКе на момент проведения контрольной проверки, является подтверждением верности/неверности ЭП Клиента под ЭД.

Приложение №6
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

ПОРЯДОК ОБМЕНА МЕЖДУ БАНКОМ И КЛИЕНТОМ В ЭЛЕКТРОННОМ ВИДЕ ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ, СВЯЗАННЫМИ С ПРОВЕДЕНИЕМ ВАЛЮТНЫХ ОПЕРАЦИЙ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предметом настоящего Порядка являются взаимоотношения Сторон по обмену в электронном виде документами и информацией, требование о представлении (направлении) которых предусмотрено законодательством Российской Федерации, в том числе нормативными актами Банка России, регламентирующими порядок осуществления функций агента валютного контроля (далее – документы валютного контроля).

1.2. Стороны соглашаются, что документы валютного контроля, направляемые по Системе «Интернет Банк-Клиент», подписываются усиленной неквалифицированной электронной подписью и признаются равнозначными документам на бумажном носителе, подписанным собственноручными подписями уполномоченных Сторонами лиц и заверенным печатью.

2. ПОРЯДОК ФОРМИРОВАНИЯ И ПЕРЕДАЧИ ДОКУМЕНТОВ И ИНФОРМАЦИИ

2.1. Формализованные документы валютного контроля, указанные в Приложении №3 к Договору, формируются Сторонами в электронном виде с использованием программно-технических средств Системы «Интернет Банк-Клиент» и подписываются электронной подписью.

2.2. Документы, обосновывающие проведение валютных операций, оформление/переоформление/прием на обслуживание/закрытие паспортов сделок, а также документы, подтверждающие вывоз (ввоз) товара с территории (на территорию) Российской Федерации, выполнение работ, оказание услуг, передачу информации и результатов интеллектуальной деятельности, в том числе исключительных прав на них, предоставляются Клиентом в виде изображений документов, полученных с использованием сканирующих устройств.

Файлы изображений могут быть прикреплены как к указанным в Приложении №3 формализованным документам, так и к письму свободного формата, подписанному электронной подписью.

2.3. Ведомости контроля и паспорта сделок, предоставляемые Клиентом при переводе договоров на обслуживание в БАНК из иных уполномоченных банков, а также направляемые Клиенту при закрытии в БАНКе паспортов сделок в связи с переводом в иные уполномоченные банки, при уступке резидентом требования по контракту (кредитному договору) другому лицу - резиденту либо при переводе долга резидентом по контракту (кредитному договору) на другое лицо – резидента, должны быть сформированы в виде файлов установленного Банком России формата XML. Для передачи по Системе «Интернет Банк-Клиент» файлы прикрепляются к письму свободного формата, подписанному электронной подписью.

2.4. Направление Сторонами запросов, разъяснений и иной информации, необходимой для целей валютного контроля, осуществляется посредством передачи писем свободного формата, подписанных электронной подписью.

2.5. Датой предоставления документов, направленных Клиентом по Системе «Интернет Банк-Клиент» в рамках установленного БАНКом операционного дня, считается текущая дата.

При направлении Клиентом по Системе «Интернет Банк-Клиент» документов после окончания установленного БАНКом операционного дня, то датой предоставления данных документов считается следующий рабочий день.

2.6. Датой принятия БАНКом поступившего от Клиента ЭД является дата установления в Системе «Интернет Банк-Клиент» статуса данного документа «Исполнено» и подписания ЭП БАНКом. Датой возврата в БАНК поступившего от Клиента ЭД является дата установления в Системе «Интернет Банк-Клиент» статуса данного документа «Отвергнуто» и подписания ЭП БАНКом.

2.7. Клиент вправе отозвать направленные ранее ЭД путем направления в БАНК сообщения с учетом требований законодательства о валютном регулировании и валютном контроле.

3. ВЗАИМОДЕЙСТВИЕ СТОРОН

3.1. В рамках настоящего Порядка Клиент:

– формирует и предоставляет в БАНК по Системе «Интернет Банк-Клиент» документы и информацию, указанные в п.2.1-2.4 настоящего Порядка, в соответствии с требованиями нормативных актов Банка России, внутренних документов БАНКа и настоящего Договора;

– регулярно осуществляет сеансы связи с БАНКом с целью получения формализованных документов, подписанных электронной подписью БАНКа, с отметками о приеме/отказе в приеме электронных документов;

– в случае получения от БАНКа отказа в приеме электронных документов Клиент вправе после устранения выявленных недостатков повторно направить документы в БАНК в сроки, по возможности, не превышающие сроки, установленные Банком России для предоставления таких документов.

3.2. В рамках настоящего Порядка БАНК:

– осуществляет проверку документов, полученных по Системе «Интернет Банк-Клиент» в порядке и в сроки, предусмотренные нормативными актами Банка России, внутренними документами БАНКа и настоящим Договором;

– редактирует полученные формализованные документы в части внесения информации в разделы, предназначенные для заполнения БАНКом;

– при положительном результате проверки проставляет на формализованных документах отметку о дате приема документа БАНКом и возвращает их Клиенту в электронном виде по Системе «Интернет Банк-Клиент» в срок не позднее 2-х рабочих дней после даты приема документов;

– при отрицательном результате проверки возвращает Клиенту непринятые формализованные документы в электронном виде с указанием даты возврата и причины отказа в их принятии. БАНК отказывает Клиенту в приеме документов в сроки и по основаниям, установленным законодательством Российской Федерации, в том числе нормативными актами Банка России, внутренними документами БАНКа и настоящим Договором.

Приложение №7
к Договору на обслуживание
клиентов в Системе "Интернет Банк-Клиент"
№_____________ от "__" _______ 20_г.

ЗАЯВКА НА ПОДКЛЮЧЕНИЕ К СИСТЕМЕ "ИНТЕРНЕТ БАНК-КЛИЕНТ"

(заполняется клиентом)	
1. Наименование организации	
2. Руководитель	Должность: ___________ Ф.И.О. ___________
3. Вид собственности организации	☐ Государственная ☐ Муниципальная ☐ Паевая или акционерная ☐ Частная ☐ Иная ___________
4. Периодичность исходящих платежей (предположительно)	☐ Нерегулярно ☐ Еженедельно по дням: ___________ ☐ Ежедневно ☐ Ежемесячно по дням: ___________ ☐ Другая периодичность: ___________
5. Максимальное количество расчетных документов в день (предположительно)	☐ Менее 10 ☐ 10-99 ☐ 100-999 ☐ Более (сколько) __________
6. Контактные лица по бухгалтерским вопросам	1. Ф.И.О. ___________тел. ___________ 2. Ф.И.О. ___________тел. ___________
7. Каким способом Вы хотели бы получать уведомления из БАНК?	☐ По телефону: ___________ ☐ По электронной почте: ___________ ☐ Другим способом: ___________ Другая система___________
8. Укажите адрес электронной почты	(e-mail) ___________
9. Сколько сотрудников будут пользоваться системой "Интернет Банк-Клиент"?	☐ Один ☐ Больше: укажите, сколько ___________

10. IP фильтрация (необходимо выбрать первый или второй пункт)	
1. Просим не ограничивать доступ в систему Интернет Банк-Клиент определенными IP адресами [возможно только в том случае, когда у клиента все действующие ключи ЭЦП сгенерированы на USB-токене(ах)]	☐
2. Просим ограничить доступ в систему Интернет Банк-Клиент только следующими IP адресами	☐
№/№	IP адрес
11. Просим выдать USB-токен (-ы) в количестве:	____________________ штук
Уполномочиваю ЦМРБанк (ООО) осуществить списание денежных средств в оплату за оказание услуги криптографической защиты путем безакцептного списания денежных средств в размере _______________ руб., согласно тарифам со счета №_________________________.	
12. Блокировочное слово:	

Информация об обслуживании клиента (заполняется сотрудниками отделения/филиала)	
1. Отделение БАНКа	
2. Руководитель БАНКа	Ф.И.О. ___________ тел. ___________
3. Специалист	Ф.И.О. ___________ тел. ___________
4. Код клиента в операционном дне	

5. Счета клиента и права доступа к ним	Счета клиента	Права доступа к указанным счетам	
		полное распоряжение счетом	просмотр и получение выписок по счету
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐
	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐	☐

6. Срок подключения к системе "Интернет Банк-Клиент"	"_____" __________ 200___ г.

7. Настоящее заявление является неотъемлемой частью Договора № ____ на обслуживание клиентов в системе «Интернет Банк-Клиент» от «___»__________20___г.

Дата заполнения: "_____" __________200 ___ г.
Руководитель Банка "________________"_____________________/______________/
Клиент "_____________________________________"________________ ______/______________/

Приложение №8
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ «ЦМР Бизнес»

1.1. Доступ в Систему «Интернет Банк-Клиент» может осуществляться Клиентом в том числе с Мобильных устройств через Мобильное приложение. Для доступа к Системе «Интернет Банк-Клиент» через Мобильное приложение необходимо оформить «Заявлении на подключение/отключение к Мобильному приложению «ЦМР Бизнес»» (Приложение №9 к настоящему Договору) и установить его на свое Мобильное устройство.

1.2. Работа в Мобильном приложении возможна только при условии подключения Клиента к Системе «Интернет Банк-Клиент».

1.3. Мобильное приложение доступно для устройств на платформах Android (версия 5.0 и выше). С целью расширения функциональных возможностей Мобильного приложения Банк имеет право по своему усмотрению периодически выпускать обновления Мобильного приложения. Клиент самостоятельно выбирает режим установки обновлений на Мобильное устройство.

1.4. Для регистрации в Мобильном приложении используется номер мобильного телефона, указанный в «Заявлении на подключение/отключение к Мобильному приложению «ЦМР Бизнес»» (Приложение №9 к настоящему Договору). Дополнительно с целью повышения удобства и скорости использования Мобильного приложения может быть настроен вход по ПИН коду или иному доступному в Мобильном устройстве способу аутентификации. Настройка входа по ПИН коду настраивается пользователем самостоятельно.

1.5. Мобильное приложение дает доступ ко всей функциональности Системы «Интернет Банк-Клиент». Состав банковских услуг, предоставляемых посредством Мобильного приложения и функциональность Мобильного приложения определены Руководством пользователя по работе в Мобильном приложении «ЦМР Бизнес», размещенном на сайте странице Интернет-банка, по адресу: https://ibank.cmrbank.ru/ibank2.

1.6. Устанавливая Мобильное приложение на свое Мобильное устройство и вводя Аутентификационные данные, пользователь подтверждает свое согласие на использование Мобильного приложения.

1.7. Подписание документов в Мобильном приложении осуществляется с помощью облачной ЭП. Ограничения, установленные Договором на обслуживание клиентов в Системе «Интернет Банк-Клиент» для ЭП, также действуют и для Мобильного приложения.

1.8. Права и обязанности Сторон при работе с Мобильным приложением определяются условиями на обслуживание клиентов в Системе «Интернет Банк-Клиент».

1.9. Клиент уведомлен о необходимости до начала работы в Мобильном приложении ознакомиться с Рекомендациями по обеспечению информационной безопасности при использовании Мобильного приложения (Приложение №10 к Договору). Использование Мобильного приложения влечет за собой дополнительный риск мошеннических действий третьих лиц, в том числе в случае, если используется одно устройство для работы и получения кодов аутентификации.

1.10. В целях обеспечения безопасности работы Мобильного приложения, Банк оставляет за собой право не предоставлять (блокировать) доступ к приложению с использованием отдельных версий операционных систем, не отвечающих требованиям информационной безопасности. Доступ к Мобильному приложению прекращается при расторжении Договора на обслуживание клиентов в Системе «Интернет Банк-Клиент».

1.11. Банк может получать данные Мобильного устройства, на котором установлено Мобильное приложение в порядке, установленном в Приложении №11 к Договору - «Политика конфиденциальности при использовании Мобильного приложения».

Приложение №9
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

ЗАЯВЛЕНИЕ
НА ПОДКЛЮЧЕНИЕ / ОТКЛЮЧЕНИЕ
К МОБИЛЬНОМУ ПРИЛОЖЕНИЮ «ЦМР Бизнес»

_____, ИНН _____
(указывается полное наименование организации/ФИО индивидуального предпринимателя, ИНН)

в лице _____
(должность)

_____,
(Ф.И.О.)

действующего на основании _____

просит Вас:

☐ Подключить к Услуге

☐ Отключить от Услуги

Номер мобильного телефона	Вид подключения Услуги (нужное отметить)	
_____		Информационный[3]
		Полнофункциональный[4]

С Тарифами и условиями обслуживания в ЦМРБанк (ООО) ознакомлен и полностью согласен.

Руководитель организации / Индивидуальный предприниматель

_____ _____ _____

М.П.

Дата: «_____» _____20 ___ г.

Заполняется работником Банка

Заявление проверено и принято к исполнению.

Дата: «_____» _____20 ___ г.

_____ _____ _____

М.П.

[3] Мобильное приложение доступно на просмотр информации.
[4] Полный доступ к Мобильному приложению, создание, подписание и подтверждение писем / платежных документов.

Приложение №10
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

1. Общие рекомендации:

- Не оставляйте Мобильное устройство без присмотра.
- Настройте блокировку экрана Мобильного устройства. При включении Мобильного устройства или при выходе из спящего режима блокировку необходимо будет снимать. Для этого потребуется ввести PIN-код, пароль, графический ключ или отпечаток пальца (наличие или отсутствие представленных способов снятие блокировки Мобильного устройства зависит от конфигурации вашего устройства). Рекомендуется использовать совместно с ограничением неверных попыток снятия блокировки Мобильного устройства.
- Используйте шифрование. Средствами операционной системы Мобильного устройства зашифруйте данные, которые хранятся на устройстве.
- Используйте только лицензионное программное обеспечение.
- Не устанавливайте на Мобильное устройство программное обеспечение, полученное из неизвестных источников.
- На Мобильном устройстве всегда должны быть установлены все официальные обновления операционной системы и приложений.
- Не подключайте Мобильное устройство к чужим компьютерам и не заряжайте телефон в публичных местах зарядки мобильных устройств.

2. Дополнительные рекомендации для мобильных устройств с операционной системой Android:

- Используйте операционную систему Android версий 5.0 и выше.
- Отключите «Режим разработчика». Если был активирован режим разработчика и после этого включен режим отладки по USB, отключите его.
- Мобильное устройство не должно иметь прав суперпользователя (root) для приложений.
- Установите на Мобильном устройстве Антивирусную защиту.
- Отключите возможность установки программного обеспечения из неизвестных источников.

Приложение №11
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г.

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

1. Сфера применения и цель публикации

Настоящая Политика действует в отношении всей информации, относящейся к данным Мобильного устройства, на котором установлено Мобильное приложение, которую Банк может получить в процессе использования Мобильного приложения.

Банк собирает и обрабатывает только ту информацию, которая необходима для предоставления и оказания услуг.

Использование Мобильного приложения осуществляется на основании договоров и соглашений с Банком, которые в числе прочего регулируют все вопросы обработки и хранения Банком информации.

Настоящая Политика применима только к Мобильному приложению. Банк не контролирует и не несет ответственность за информацию (последствия её передачи), переданную пользователем третьей стороне, в случае если такая передача была выполнена на ресурсе третьей стороны, на который пользователь мог перейти по ссылкам из Мобильного приложения.

Целью настоящей Политики является информирование Клиента об условиях обработки данных Мобильного устройства при использовании Мобильного приложения.

2. Основания для обработки персональных данных

Банк собирает и хранит только ту информацию пользователя, которая необходима для предоставления сервисов, входящих в состав Мобильного приложения.

3. Состав обрабатываемых данных Мобильного устройства, на котором установлено Мобильное приложение

В процессе использования Мобильного приложения Банк может собирать разные виды информации об использовании Мобильного устройства, на котором установлено Мобильное приложение, в том числе сведения об оборудовании и программном обеспечении. К указанным сведениям относятся:

- Идентификаторы программного обеспечения, Мобильного приложения, субъекта данных и среды (идентификаторы устройств, IMSI, IMEI, идентификаторы прошивки устройства, идентификаторы установки программного обеспечения, версии программного обеспечения, операционная система, идентификатора пользователя Мобильного приложения);
- Данные об использовании функционала аутентификации на Мобильном устройстве по отпечатку пальца (данные о поддержке данного функционала Мобильным устройством, данные об активации/деактивации функционала, данные о факте смены отпечатка пальца, используемого для аутентификации на Мобильном устройстве);
- Данные об установленных Мобильных приложениях (имена файлов, имена пакетов, пути, разрешения, сертификаты, источник, используемые библиотеки, дата и время установки, репутация приложения);
- Данные о местоположении Мобильного устройства (координаты, точность координат);
- Активные сетевые подключения (GPRS, GPS, Wi-Fi);
- Роуминг Мобильного устройства;
- Данные о сетевых подключениях (IP-адреса, MAC-адреса, URL-адреса, данные HTTP-реферера, SSID, VPN подключения);
- Отпечаток свойств Мобильного устройства (свойства прошивки и оборудования устройства, характеристики дисплея, свойства датчиков, данные сетевого подключения, текущие настройки, текущие настройки безопасности, местоположение, системные настройки, настройки webView, данные webGI, отпечаток);
- Данные о файлах (размер, имя, путь, хэш-сумма файла, MD5);
- Данные SensorEvent;

4. Цели обработки данных Мобильного устройства, на котором установлено Мобильное приложение

Банк обрабатывает данные Мобильного устройства для достижения следующих целей:

- **Обеспечение безопасности.** Банк обеспечивает безопасность в Мобильном приложения и конфиденциальность данных Мобильного устройства. Для этого Банк использует собранные сведения для разработки обновлений и исправлений систем безопасности. Для достижения этой цели Банк использует сведения о Мобильном устройстве и об использовании Мобильного приложения.

- **Предотвращение мошеннических действия**. Банк обеспечивает безопасность операций в Мобильном приложении. Для этого Банк использует сведения о Мобильном устройстве и использовании Мобильного приложения.

5. Способы обработки и действия, совершаемые с данными Мобильного устройства, на котором установлено Мобильное приложение

Банк осуществляет обработку и хранение информации в соответствии с внутренними регламентами и правилами безопасной обработки данных, с сохранением ее конфиденциальности. При обработке данных Мобильное приложение не раскрывает личность пользователя третьим лицам.

При обработке идентификационных и платежных данных Мобильное приложение ни при каких обстоятельствах не публикует/не распространяет персональную информацию, личные и конфиденциальные данные пользователя.

Информация может быть предоставлена государственным органам по запросу в соответствии с требованиями законодательства Российской Федерации.

Действия, совершаемые Банком с данными Мобильного устройства: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

6. Меры для защиты данных пользователя

Банк принимает все зависящие от Банка организационные и технические меры для защиты информации пользователя от неправомерного или случайного доступа третьих лиц, уничтожения, изменения, блокирования, использования, копирования и распространения, от иных неправомерных действий.

Приложение №12
к Договору на обслуживание
клиентов в Системе “Интернет Банк-Клиент”
№_____ от “__” _____ 20_г

Заявление на выпуск сертификата ключа проверки ЭП

Банку_____

От Клиента_____

Просим выпустить сертификат ключа проверки ЭП в соответствии с идентификационными данными:

1.Сведения об организации		
1.1	Наименование организации	
1.2	Место нахождения	
1.3	ОГРН	
1.4	Дата внесения в ЕГРЮЛ (ЕГРИП)	
1.5	ИНН (КИО)	
1.6	КПП	
1.7	Телефон	
2.Сведения о владельце ключа		
2.1	ФИО	
2.2	Должность	
2.3	Документ, удостоверяющий личность	
2.4	Серия	
2.5	Номер	
2.6	Дата выдачи	
2.7	Кем выдан	
2.8	Код подразделения	
3.Сведения о ключе проверки ЭП		
3.1	Идентификатор	
3.2	Наименование криптосредств	
3.3	Идентификатор устройства	
3.4	Алгоритм	
3.5	ID набора параметров алгоритма	
3.6	Представление ключа проверки ЭП	
3.7	Срок действия	

_____ Дата создания ключа ЭП: _____
_____