

Договор присоединения
на обслуживание в системах дистанционного банковского обслуживания

Настоящая форма Договора является стандартной (типовой) формой. Условия настоящего Договора определены в стандартной форме и могут быть приняты Клиентом не иначе как путем подписания Заявления на подключение к системе «Onlinebank HALYK» и о присоединении к договору по форме в Приложении 1 к Условиям Onlinebank» (далее – Система Onlinebank) или по форме Заявления на подключение к системе «Интернет-банкинг для юридических лиц» и о присоединении к договору по форме Приложения к Условиям Correqts (далее – Система Correqts). Договор является Договором присоединения, заключаемым в соответствии с действующим законодательством Республики Казахстан и внутренними документами Банка. При этом Заявления на подключение к Системам и Договор рассматриваются только в качестве единого документа.

Клиент присоединяется к Договору путем подписания Заявления по форме приложения. Подпись Клиента, его представителя(-ей) на Заявлении означает, что Клиент ознакомлен с условиями предложенного ему Банком Договора, включая приложения к Договору, и принимает их не иначе как путем присоединения к Договору, размещенному по электронному адресу: www.halykbank.kz, в целом.

Настоящий Договор устанавливает права, обязанности, ответственность Сторон и иные правоотношения между Банком и Клиентом, определяет условия и порядок оказания Банком услуг при подключении Клиента к Системам, оказанию платежных услуг Клиенту, совершения Клиентом операций по текущему банковскому счету посредством Систем и предоставления дополнительных услуг, связанных с Системами.

Статья 1. Предмет Договора

1.1. Предметом Договора является предоставление Банком банковских услуг посредством Систем, при условии оплаты Клиентом данных услуг на условиях Банка.

1.2. Стороны признают, что используемые при совершении операций в Системах и/или посредством Мобильного приложения документы в электронной форме (далее – электронные документы), подписанные электронной цифровой подписью (далее – ЭЦП) и/или одним из Способом динамической аутентификации равнозначны документам на бумажном носителе и порождают аналогичные им права и обязанности Сторон по настоящему Договору.

1.3. Стороны признают, что каждая из Сторон может в электронной форме передавать другой Стороне или получать от другой Стороны документы, сообщения (указания), указанные в Договоре.

1.4. Клиент признает, что обмен Электронными документами возможен только при наличии у отправителя Ключевого носителя, регистрационного свидетельства, прошедших проверку в удостоверяющем центре, и/или Способа динамической аутентификации.

1.5. Стороны признают используемую ими по настоящему Договору систему защиты информации достаточной для защиты от несанкционированного доступа, а также подтверждения авторства и подлинности Электронных документов, направляемых Клиентом с использованием Ключевого носителя и/или Способа динамической аутентификации.

1.6. Клиент признает, что при подписании Заявления на подключение к системе «Onlinebank HALYK» он соглашается с Условиями обслуживания через Систему «Onlinebank HALYK» согласно Приложению 1 к Договору, а при подписании Заявления на подключение к системе «Интернет-банкинг для юридических лиц» он соглашается с Условиями обслуживания через Систему «Интернет-банкинг для юридических лиц» согласно Приложению 2 к Договору.

Статья 2. Используемые термины

2.1. Термины, используемые в настоящем Договоре с заглавной буквы, имеют толкование, которое дано им в Договоре, если иное толкование не содержится непосредственно в тексте.

«Onlinebank HALYK» (далее – Система Onlinebank) –	Система услуг Банка, предоставляющая Клиенту возможность дистанционного управления своими банковскими счетами, открытыми в Банке путём обмена Электронными документами, сообщениями (указаниями) между Клиентом и Банком через сеть интернет.
«Onlinebank Business» –	Версия Системы Onlinebank, предоставляющая Клиенту возможность дистанционного управления своими банковскими счетами, открытыми в Банке путём обмена Электронными документами, сообщениями (указаниями) между Клиентом и Банком через сеть интернет без ограничения Клиента по количеству и/или сумме в отправленных Электронных документах на исполнение в Банк.
«Onlinebank Start» –	Версия Системы Onlinebank, предоставляющая Клиенту возможность дистанционного управления своими банковскими счетами, открытыми в Банке путём обмена Электронными документами, сообщениями (указаниями) между Клиентом и Банком через сеть интернет с установленным Банком ограничением (лимитом) Клиента по количеству и/или сумме в отправленных Электронных документах на исполнение в Банк. Информация по лимитам размещена по электронному адресу: в разделе Бизнес – Транзакционное обслуживание - Расчетно-кассовое обслуживание на сайте www.halykbank.kz Увеличение лимита может быть рассмотрено Банком при оплате Клиентом данной услуги по Тарифам Банка, указанных на сайте www.halykbank.kz
Onlinebank-аутентификация –	Мобильное приложение, установленное на мобильное устройство, которое позволяет Клиенту самостоятельно по запросу генерировать уникальную последовательность электронных цифровых символов (далее – Код), предназначенную для одноразового использования при входе в Систему Onlinebank или Мобильное приложение, и/или авторизации электронных платежей. При каждом входе Клиента в Систему Onlinebank и/или авторизации платежей требуется создание и использование нового одноразового (единовременного) кода.
Pin-код –	Секретный код, известный только уполномоченному лицу Клиента, на имя которого выдано Регистрационное свидетельство. Pin-код обеспечивает возможность использования Ключевого носителя в системе Onlinebank только лицом, знающим Pin-код.
SMS-аутентификация –	Услуга по получению SMS сообщение от Банка, которое содержит сгенерированную уникальную последовательность электронных цифровых символов (далее – Код), предназначенную для одноразового использования при входе в Систему Onlinebank или Мобильное приложение, и/или авторизации электронных платежей. При каждом входе Клиента в Систему и/или авторизации платежей требуется создание и использование нового одноразового (единовременного) кода. На SMS-аутентификацию платежей Банк может установить суточный лимит. Информация по лимитам и размер размещена по электронному адресу: www.halykbank.kz
SMS-информирование –	Услуга, предоставляемая Банком для информирования Клиента об операциях по текущим счетам и предоставление выписок по банковскому счету/счетам путем отправки SMS-сообщений Банком на Доверенный номер Клиента. Услуга предоставляется лишь для пользователей Системы Onlinebank. Размер комиссионного вознаграждения за подключение к Услуге определяется согласно Тарифам Банк на сайте www.halykbank.kz .

SMS-уведомление –	Услуга, предоставляемая Банком для информирования Клиента об исходящих платежах и переводах Клиента, произведенных в тенге с текущих счетов Клиента, открытых в Банке, путем отправки SMS-сообщения на номер мобильного телефона уполномоченного лица (работника) Клиента с текстом следующего содержания: «HalykBank, schet XXXX, iniciirovan platezh, summa XXXX,XX KZT, дд.мм.гг чч:мм:сс; platezh budet proveden cherez XX min, ContactCenter №XXXXXXXXXX».
Банк –	АО «Народный Банк Казахстана», включая его филиалы.
Выписка –	Надлежащим образом оформленный документ (на бумажном носителе или в электронной форме) о состоянии Счета Клиента за определенный период времени.
Действующее законодательство –	Законодательство Республики Казахстан, состоящее из нормативных правовых актов, принятых в установленном порядке.
Деньги –	Средство платежа, выраженное в национальной или иностранной валюте.
Доверенный номер –	Номер мобильного (сотового) телефона, предоставленный Клиентом Банку, способами, определяемыми Банком самостоятельно и используемый Клиентом для получения электронных банковских услуг с использованием Динамической идентификации клиента.
Договор –	Договор присоединения на обслуживание в системах дистанционного банковского обслуживания
Закрытый ключ ЭЦП –	Последовательность электронных цифровых символов, созданная Клиентом на ключевом носителе в процессе регенерации посредством Систем, зарегистрированная в удостоверяющем центре и известная только владельцу регистрационного свидетельства, предназначена для создания ЭЦП с использованием средств криптографической защиты информации. В случае утери или компрометации закрытого ключа ЭЦП Клиент обязан в кратчайшие сроки предоставить в Банк или удостоверяющий центр заявление на отзыв ключа ЭЦП и регистрационного свидетельства к нему.
Карт-ридер –	Электронно-механическое устройство, обеспечивающее взаимодействие используемого уполномоченным лицом Клиента оборудования с чипом в Ключевом носителе в целях создания Электронных документов с использованием его ЭЦП на применяемом им оборудовании.
Клиент –	Юридическое лицо либо обособленное подразделение юридического лица (филиал, представительство), индивидуальный предприниматель, частный нотариус, частный судебный исполнитель, адвокат, профессиональный медиатор, ликвидируемый банк, страховая (перестраховочная) организация, их филиал – резиденты Республики Казахстан, иностранное дипломатическое и консульское представительство, заключившее настоящий Договор.
Ключевой носитель –	Защищенное электронное устройство, предназначенное для генерации, хранения закрытого и открытого ключей ЭЦП и выполнения криптографических операций с использованием средств криптографической защиты информации.
Ключи первичной инициализации –	Криптографические ключи, используемые Клиентом для начала работы с Системой, предназначенные для замены на криптографические ключи ЭЦП посредством Системы.

Колбэк (callback) –	Звонок из Банка Клиенту о необходимости подтверждения транзакции. Для подтверждения транзакции Клиент называет «кодовое слово» и детали транзакции.
Логин и пароль –	Уникальный набор букв и/или цифр (символов), используемый пользователями для доступа к Системе Correqts. При этом логин и пароль является конфиденциальным и не должны передаваться пользователями третьим лицам.
Мобильное приложение (МП) –	Приложение, установленное на Мобильном устройстве Клиента для работы в Системе. При работе через данное приложение применяются лимиты по суммам в Системе на совершение операций.
Мобильное устройство –	Планшетный компьютер, смартфон или фаблет с установленными операционными системами iOS или Android.
Мобильный бизнес-клиент (МБК)	Подсистема, позволяющая Клиентам получать доступ к Системе Correqts через Мобильные устройства.
Операционный день –	Часы, установленные Банком для приема платежных документов, осуществления кассовых операций и иных операций.
Открытый ключ ЭЦП –	Последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности ЭЦП в электронном документе.
Платформа «Halyk FX» –	Дополнительный раздел Системы, который предоставляет Клиенту индивидуальный курс для сделок по конвертациям валюты на условиях, определяемых Банком.
Подписывающее лицо –	Физическое, правомерно владеющее закрытым ключом ЭЦП и обладающее правом на его использование в Электронном документе.
Процедура безопасности –	Комплекс организационных мер и программно-технических средств защиты информации, предназначенных для идентификации и авторизации Клиента при составлении, передаче и получении электронных документов, сообщений (указаний) с целью установления его права на получение электронных банковских услуг, а также для обеспечения конфиденциальности и обнаружения ошибок и/или изменений в содержании передаваемых и получаемых электронных документов, сообщений (указаний).
Рабочая станция –	Оборудование, к которому подключается карт-ридер или Java Token и/или осуществляется вход и авторизация Клиента в Системе.
Рабочие дни –	Дни, когда банки в Республике Казахстан и/или стране происхождения соответствующей иностранной валюты открыты для совершения сделок.
Регистрационное свидетельство –	Документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия открытого ключа ЭЦП закрытому ключу ЭЦП и требованиям, установленным Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи».
Регистрационное свидетельство первичной инициализации –	Документ на бумажном носителе или электронный документ, передаваемый Банком Клиенту для начала работы с Системой, предназначенный для получения посредством Системы в удостоверяющем центре регистрационного свидетельства на ключи ЭЦП.
Способ динамической аутентификации –	Выбранный Клиентом способ получения одноразового (единовременного) кода, которым Клиент подтверждает вход в систему и/или отправку в Банк Электронного документа. Способом динамической аутентификации являются: Onlinebank-

	аутентификация, SMS-аутентификация, аутентификация с помощью Устройства eToken PASS.
Система «Интернет-банкинг для юридических лиц» (далее – Система Correpts)	Система услуг Банка, предоставляющая Клиенту возможность дистанционного управления своими банковскими счетами, открытыми в Банке путём обмена электронными документами, сообщениями (указаниями) между Клиентом и Банком через сеть интернет (модуль «Интернет-Клиент») и/или через модемный пул Банка (модуль «Банк-Клиент») и/или подсистему Мобильный бизнес-клиент.
Системы дистанционного банковского обслуживания (далее - Системы)	Системы Банка, предоставляющая Клиенту возможность дистанционного управления своими банковскими счетами, открытыми в Банке. Включает в себя Систему Onlinebank и Систему Correpts.
Сторона/Стороны	Банк и Клиент, заключившие Договор.
Счет	Банковский счет Клиента в Банке в любой валюте, открытый на основании Договора банковского счета, Договора банковского вклада. Здесь учитываются также случаи, когда по Договору банковского счета открывается один или несколько счетов.
Тарифы	Тарифы, определяющие размеры комиссий Банка за оказываемые им Клиенту услуги, размещенные на интернет-сайте Банка www.halykbank.kz .
Удостоверяющий центр –	Юридическое лицо, имеющее договорные отношения с Банком и/или подразделение Банка, удостоверяющее соответствие открытого ключа ЭЦП закрытому ключу ЭЦП, а также подтверждающее достоверность и активность регистрационного свидетельства.
Уполномоченное лицо/ Уполномоченный представитель	Лицо, наделенное полномочиями в соответствии с действующим законодательством и выступающее от имени Клиента, Банка или третьих лиц, как предусмотрено Условиями и/или Договором.
Уполномоченный орган	Национальный Банк Республики Казахстан или иной уполномоченный государственный орган.
Уровень безопасности	Выбираемая Клиентом степень защищенности данных при работе в Системе Onlinebank В Банке действуют следующие Уровни безопасности, которые включают в себя комбинацию различных средств и мер защиты, в зависимости от уровня: 1) «Высокий» Уровень безопасности – подключение к Системе версией «Onlinebank HALYK Business» и использование при работе с Системой Ключевого носителя и Способа динамической аутентификации 2) «Средний» Уровень безопасности – подключение к Системе версией «Onlinebank HALYK Business» и использование при работе с Системой только Смарт-карты 3) «Низкий» Уровень безопасности – подключение к Системе версией «Onlinebank HALYK Start» и использование при работе с Системой только SMS и Onlinebank-аутентификация
Условия Onlinebank	Условия, описывающие обслуживание Клиента через Систему «Onlinebank HALYK», указанные в Приложение 1 к Договору
Условия Correpts	Условия, описывающие обслуживание Клиента через Систему «Интернет-банкинг для юридических лиц» версии Correpts или ДБОЗ, указанные в Приложение 2 к Договору
Устройства для аутентификации –	При использовании данного термина, подразумеваются все выданные Клиенту устройства при подключении Систем, указанные Клиентом в Заявление на подключение Систем. Банком могут выданы следующие устройства:

	1) Ключевой носитель (Java Token или смарт-карта) 2) Карт-ридер (выдается в случае использования Ключевого носителя на смарт-карте) 3) Устройство eToken PASS
Устройство eToken PASS –	Самостоятельное устройство, позволяющее Клиенту самостоятельно по запросу генерировать уникальную последовательность электронных цифровых символов (далее – Код), предназначенную для одноразового использования при входе в Системы и/или авторизации электронных платежей. При каждом входе Клиента в Системы требуется создание и использование нового одноразового (единовременного) кода.
Электронная цифровая подпись (далее – ЭЦП) –	Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость). Допускается проставление под электронными документами одной и более электронных подписей, принадлежащих Клиенту и прошедших проверку в удостоверяющем центре. Допускается проставление под электронными документами одной и более электронных подписей, принадлежащих Клиенту и прошедших проверку в удостоверяющем центре.
Электронный документ –	Документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством ЭЦП.

Статья 3. Обеспечение безопасности

3.1. Клиент соглашается следовать процедурам безопасности и любым другим инструкциям, предоставляемые Банком Клиенту относительно безопасности Системы.

3.2. Клиент принимает на себя полную ответственность за установку, поддержание и регулярный контроль за организацией безопасности и использования Устройств для аутентификации, а также информации, хранимой в его компьютерных и коммуникационных системах, мобильных устройствах, и, в частности, контроль за паролями для входа в Системы.

3.3. Клиент обязуется незамедлительно уведомлять Банк о любом несанкционированном доступе к Системам, в том числе к Мобильному приложению, к его Рабочей станции или несанкционированной операции, о которых он знает или подозревает.

3.4. Клиент соглашается оградить Банк от всех исков и судебных разбирательств, возместить Банку издержки, убытки и ущерб любого типа, которым Банк может быть подвержен в результате неисполнения или ненадлежащего исполнения Клиентом своих обязательств согласно настоящей статье.

3.5. Клиент обязуется бережно относиться к следующим устройствам:

- Ключевому носителю, в случае подключения Систем с его использованием;
- Карт-ридеру, в случае выбора Ключевого носителя – смарт-карты;
- Устройство eToken PASS, в случае выбора Клиентом данного Способа динамической аутентификации.

А также избегать механических воздействий (падения, сотрясения, вибрации и т.д.), самостоятельно не разбирать, оберегать от резких перепадов температуры, от попадания пыли, грязи, влаги, не подвергать высокому напряжению и другим факторам, которые могут негативно сказаться на работе вышеуказанных устройств.

3.6. Клиент подтверждает, что Ключевой носитель и/или Карт-ридер подключается лишь к исправному оборудованию (USB-порты, USB-хабы с дополнительным питанием), извлекается правильно, не остается подключенным к компьютеру при выключении, перезагрузке и уходе в спящий режим.

Статья 4. Услуги SMS-уведомление и SMS-информирование

4.1. Для получения информации о платежах посредством SMS-уведомления на мобильный телефон Клиент заполняет заявление по форме Приложения 4 к Договору о подключении данной услуги. Для получения информации о платежах посредством SMS-информирования на Доверенный номер, Клиент самостоятельно направляет запрос на подключение посредством Системы Onlinebank.

4.2. SMS-уведомления и SMS-информирование о платежах передаются посредством сетей телекоммуникаций, предоставляемых операторами сотовой связи Казахстана в рамках отдельных соглашений с Банком, предусматривающих соблюдение операторами требований конфиденциальности информации клиентов Банка.

4.3. Настоящим Клиент дает согласие Банку на раскрытие оператору сотовой связи Казахстана сведений, составляющих банковскую тайну Клиента, которыми Банк обладает на законных основаниях, необходимых для подключения Клиента к услугам SMS-уведомление и SMS-информирования и передачи SMS-сообщений в рамках данных услуг. При этом Клиент заверяет, что настоящее письменное согласие Банку на раскрытие сведений, составляющих банковскую тайну, предоставлено в Банк, при подписании заявления по форме Приложения 4 к Договору при подключении к услуге SMS-уведомления и/или при подписании заявления по форме Приложения 2 к Условиям Onlinebank при подключении к услуге SMS-информирование уполномоченным лицом Клиента в момент его личного присутствия в порядке, установленном Действующим законодательством.

4.4. При подключении Услуги SMS-уведомления Клиент обязан:

- 1) подключиться к услуге аудиообслуживания;
- 2) предоставить Банку информацию о номерах мобильных телефонов уполномоченных лиц (работников) Клиента, подключенных к услуге SMS-уведомление, в заявлении, составленном по форме согласно Приложению 4 к Договору, на бумажном носителе либо посредством Системы;
- 3) уведомить Банк об изменении номера мобильного телефона либо прекращении полномочий лиц, указанных в заявлении, составленном по форме согласно Приложению к Условиям Onlinebank, не менее чем за 5 (пять) рабочих дней. Клиент настоящим дает согласие Банку на раскрытие лицам, указанным в заявлении, у которых прекращены полномочия, но о чем Банк не получил от Клиента соответствующего уведомления, сведений, относящихся к банковской тайне, которые указываются в SMS-уведомлении. При этом Клиент заверяет, что настоящее письменное согласие Банку предоставлено в Банке при подписании заявления по форме Приложения к Условиям Onlinebank о подключении данной услуги уполномоченным лицом Клиента в момент его личного присутствия в порядке, установленном действующим законодательством;
- 4) сообщать Банку в течение времени, указанного в SMS-сообщении, о платежах, не инициированных Клиентом, только по номеру телефона, указанному в SMS-сообщении;
- 5) производить оплату предоставления услуги SMS-уведомление согласно тарифам Банка.

Статья 5. Обязанности и права Сторон. Персональные данные. Комиссионное вознаграждение Банка

5.1. Стороны обязуются:

- использовать системы телекоммуникаций, обработки, хранения и защиты информации только на работоспособном и исправном оборудовании, проверенном на отсутствие компьютерных вирусов и программ, способных нанести вред Системам и Сторонам;
- не разглашать третьей стороне (за исключением случаев, предусмотренных действующим законодательством или дополнительным соглашением Сторон) конкретные способы защиты информации, применяемые в Системах, а Банк также не разглашать информацию, полученную от Клиента при предоставлении электронных банковских услуг, за исключением случаев разглашения информации, предусмотренных Действующим законодательством;
- один раз в год (за 30 календарных дней до истечения срока действия) проводить смену закрытого ключа ЭЦП и регистрационного свидетельства посредством Систем, а в случае, когда смена не была произведена до истечения срока действия, то Клиент обращается в Банк для повторного перевыпуска на платной основе согласно тарифам Банка;
- немедленно информировать другую Сторону обо всех случаях подозрений на несанкционированный доступ в системы телекоммуникаций и к закрытому ключу ЭЦП, мобильному устройству, а также обо всех случаях утраты, хищения Устройств для аутентификации, или повреждения программно-технических средств систем телекоммуникаций, обработки, хранения и защиты информации для проведения смены ключей, пароля и других согласованных с

другой Стороной действий по поддержанию в рабочем состоянии вышеуказанных программно-технических средств;

- в случае компрометации Клиентом своего закрытого ключа ЭЦП, Клиент должен обратиться в Банк с заявлением на отзыв регистрационного свидетельства, а Банк по получении письменного обращения должен немедленно отозвать регистрационное свидетельство в удостоверяющем центре;

- в случае получения письменного уведомления со стороны Клиента о подозрении на несанкционированный доступ в Системы, выявления подозрений на несанкционированный доступ к Рабочей станции Клиента и/или мобильному устройству Клиента, Банк должен немедленно блокировать все операции с электронными документами, сообщениями (указаниями), до выяснения всех обстоятельств;

- обеспечивать конфиденциальность информации, содержащейся в электронных документах, сообщениях (указаниях), в процессе предоставления и получения электронных банковских услуг.

5.2. Банк имеет право:

- отказать в приеме электронных документов к исполнению по основаниям, предусмотренным в пунктах в Условиях к Договору;

- не принимать к обработке электронные документы по основаниям, но не ограничивая себя, предусмотренным в Условиях к Договору;

- вносить изменения в механизмы защиты Систем по своему усмотрению;

- вносить изменения с Уровни безопасности и перечень необходимых устройств Ключевого носителя и/или Способа динамической аутентификации;

- без какого-либо дополнительного согласия Клиента вносить изменения в перечень документов, необходимых для работы в Системах;

- блокировать доступ Клиента в Системы в случае истечения срока действия регистрационного свидетельства Клиента;

- блокировать доступ Клиента в Системы в случае отсутствия движений по Счету и отсутствия денег на Счете Клиента в течение трёх месяцев подряд (по текущим счетам). В случае отсутствия движений по Счёту и отсутствия денег на Счете более шести месяцев подряд расторгнуть Договор путем отказа от Договора;

- блокировать доступ Клиента в Системы в случае выявления подозрительных/мошеннических операций, не подтвержденных Клиентом, по результатам проведения Банком процедуры callback (колбэк);

- блокировать доступ Клиента в Системы в случае нескольких последовательных попыток ввода неправильного Pin-кода (точное количество попыток ввода определяется Банком) и значения одноразового пароля, сгенерированного Устройством eToken PASS, SMS-аутентификацией или Mobile-аутентификацией;

- проводить любые мероприятия, направленные на повышение безопасности работы Системы путем запроса подтверждения у Клиента деталей электронных документов, сообщений (указаний), а также иными способами;

- без согласия Клиента прекратить предоставление услуги «SMS-уведомление» с предварительным уведомлением Клиента за 5 (пять) рабочих дней до планируемого прекращения предоставления услуги «SMS-уведомление»;

- в определенных случаях в зависимости от суммы платежа, вида платежа, а также других условий, которые определяются Банком самостоятельно, не направлять Клиенту SMS-сообщения по услуге «SMS-уведомление»;

- самостоятельно отключить уполномоченных лиц Клиента от Систем или от услуги «SMS-уведомление» в случае обнаружения истечения полномочий/ или увольнения указанных лиц;

- пользоваться другими правами, предусмотренными Договором.

5.3. Банк обязан:

- после заключения настоящего Договора и оплаты Клиентом надлежащих комиссий, в соответствии с тарифами Банка, зарегистрировать Клиента в выбранной Системе, передать Клиенту Ключевой носителя, логин, ПИН-конверт с паролем, в случае подключения Системы с их использованием, Карт-ридера, в случае выбора Ключевого носителя – смарт-карты и устройства

eToken PASS, в случае выбора Клиентом данного Способа динамической аутентификации, для начала работы с Системой;

- предоставить Клиенту инструктивные материалы, содержащие руководство пользователя по установке и работе с Системами;

- предоставлять электронные банковские услуги в соответствии с условиями Договора, в том числе исполнять указания Клиента на перевод денег со Счета, переданные в Банк средствами телекоммуникаций, расшифрованные и удостоверенные ЭЦП Клиента, прошедшими проверку в удостоверяющем центре и/или подтвержденные единовременным (одноразовым) кодом, сгенерированным с помощью Способа динамической аутентификации;

- предоставлять Клиенту техническую поддержку по вопросам Систем в соответствии с тарифами Банка;

- подключить номера мобильных телефонов уполномоченных лиц (работников) Клиента к услуге «SMS-уведомление» согласно заявлению, оформленному Клиентом по форме согласно Приложению 4 к Условиям;

- производить изменение регистрационной информации о номерах мобильных телефонов на основании предоставленных Клиентом письменных заявлений по форме согласно Приложению 4 к Договору.

5.4. Клиент обязан:

- изучить инструкцию по безопасности настоящего Договора и следовать описанным в ней рекомендациям Банка;

- сменить ключи первичной инициализации на действующую ключевую пару посредством Систем не позднее 30 (тридцать) календарных дней с момента подписания Договора;

- за счет собственных средств обеспечить доступ к сети интернет и самостоятельно оплачивать услуги поставщиков связи за ее использование;

- оформлять платежные документы в соответствии с действующим законодательством и настоящим Договором. Платежные поручения оформляются с проставлением обязательных реквизитов, в т.ч. в графе «код назначения платежа» – кодового обозначения платежа (КНП), соответствующего текстовому обозначению назначения платежа, а при уплате налогов и других обязательных платежей в бюджет – указывать цифровое обозначение кода бюджетной классификации (КБК), соответствующее текстовому наименованию такого кода и назначению платежа, указанному в поле «назначение платежа»;

- не модифицировать, не декомпилировать, не тиражировать и не передавать третьей стороне программно-техническое обеспечение;

- за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые в соответствии с настоящими Условиями;

- корректно отключать Ключевой носитель, в случае его выбора при использовании Системы;

- по окончании рабочей сессии в Системе – незамедлительно извлекать ключевой носитель;

- уведомить Банк о прекращении/изменении полномочий уполномоченных лиц либо их мобильных телефонов, указанных в представленных в Банк заявлениях на регистрацию пользователя в Системах, и незамедлительно отозвать их регистрационные свидетельства и отключить их услуги SMS-уведомлений в случае наличия у них такой услуги, посредством подачи заявления. Клиент настоящим дает согласие Банку на раскрытие лицам, указанным в заявлении, у которых прекращены полномочия, но о чем Банк не получил от Клиента соответствующего уведомления, сведений, относящихся к банковской тайне, которые указываются в SMS-уведомлении;

- сообщать Банку в течение времени, указанного в SMS-сообщении, о платежах, не инициированных Клиентом, только по номеру телефона, указанному в SMS-сообщении;

- осуществлять использование Системы в полном соответствии с инструкцией по эксплуатации, предоставленной Банком;

- немедленно обратиться в Банк с заявлением на отзыв регистрационного свидетельства в случае потери, раскрытия, искажения своего закрытого ключа или использования его другими лицами;

- не допускать неправомерного распространения информации о своем закрытом ключе ЭЦП;

- не разглашать Pin-код ключа ЭЦП, не указывать его на Ключевом носителе и/или не разглашать сгенерированный единовременный (одноразовый) код;
- после первого входа в Систему изменить Pin-код ключа ЭЦП и не использовать в работе стандартный Pin-код;
- принимать все возможные меры для предотвращения потери устройств Ключевого носителя и/или Способа динамической аутентификации, раскрытия, содержащейся в них информации, искажения и несанкционированного использования;
- не оставлять ключ ЭЦП без присмотра в непосредственной близости от Рабочей станции;
- не позднее чем за 30 (тридцать) рабочих дней до истечения срока действия ключей ЭЦП и регистрационного свидетельства отправить посредством Системы электронный запрос в удостоверяющий центр;
- подключиться к услуге аудиобслуживания;
- по согласованию с Банком получить ПИН-конверт с паролем, необходимым для входа в Систему Coreqts, в случае если использовавшийся Клиентом пароль был утрачен.

5.5. Клиент имеет право:

- обслуживаться в Системах в соответствии с условиями настоящего Договора;
- выбрать версию Систем, подходящую особенностям его бизнеса;
- изменять Pin-код в соответствии с требованиями к длине и сложности пароля, изложенными в инструкции по эксплуатации, предоставленной Банком;
- по согласованию с Банком, при необходимости, получить дополнительные устройства eToken PASS, Карт-ридер и/или ключевые носители;
- требовать от Банка надлежащего исполнения условий настоящего Договора.

5.6. Настоящим в соответствии с Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (далее – Закон) Клиент, представитель Клиента, подписавший Заявление, предоставляет Банку и входящим в состав финансовой Группы «Халык» (Банк и его дочерние организации (далее – Организации)) согласие на сбор и обработку Банком и (или) Организациями персональных данных Клиента, представителя Клиента, подписавшего Заявление, с целью заключения с Банком и исполнения Договора, в частности, трансграничную передачу персональных данных Клиента, представителя Клиента, подписавшего Заявление, в т.ч. согласно пп.1) п.3 ст.16 Закона, а также в иных случаях, когда в соответствии с законодательством Республики Казахстан и (или) внутренними документами Банка и (или) Организаций возникает необходимость сбора, обработки таких персональных данных. Сбор и обработка персональных данных Клиента, представителя Клиента, подписавшего Заявление, осуществляется Банком и (или) Организациями способами, не противоречащими законодательству Республики Казахстан.

5.7. Настоящим Клиент заверяет, что в отношении персональных данных субъектов персональных данных, переданных и подлежащих передаче в будущем Клиентом Банку и (или) организациям, входящим в состав финансовой Группы «Халык» (Банк и его дочерние организации (далее – Организации)), по Договору, а также в иных случаях, когда в соответствии с Действующим законодательством и (или) внутренними документами Банка и (или) Организаций возникает необходимость сбора, обработки таких персональных данных, Клиент предварительно получил у субъектов персональных данных согласия на сбор и обработку персональных данных, на передачу персональных данных третьему лицу, в т.ч. Банку и (или) Организациям, обработку Банком и (или) Организациями персональных данных.

5.8. В случае необходимости, определяемой Банком и (или) Организациями, Клиент предоставляет Банку и (или) Организациям документальное подтверждение наличия собранных Клиентом у субъектов персональных данных согласий на сбор и обработку персональных данных, на передачу персональных данных третьему лицу, в т.ч. Банку и (или) Организациям персональных данных, а при невозможности документального подтверждения наличия согласий, соберет такие согласия, а затем подтвердит Банку и (или) Организациям их получение.

5.9. Ответственность за отсутствие согласий на сбор и обработку персональных данных, на передачу персональных данных третьему лицу, в т.ч. Банку и (или) Организациям, обработку Банком и (или) Организациями персональных данных возлагается на Клиента. В случае применения к Банку и (или) Организациям каких-либо мер за нарушение законодательства Республики Казахстан о персональных данных и их защите, Клиент обязуется возместить Банку и (или)

Организациям, по требованию Банка и (или) Организаций, любые понесенные Банком и (или) Организациями расходы и убытки.

5.10. Банк вправе изымать путем прямого дебетования Счета комиссионное вознаграждение Банку за оказанные по Договору услуги в порядке и сроки, предусмотренные внутренними документами Банка.

Клиент предоставляет Банку безусловное согласие на изъятие Банком сумм комиссионного вознаграждения за оказываемые Банком по Договору услуги, а также всех затрат, понесенных Банком в связи с исполнением им по Договору указаний Клиента, путем прямого дебетования Банком Счета.

5.11. Банк вправе вносить изменения в действующие тарифы, предварительно письменно уведомив об этом Клиента за 10 (десять) рабочих дней до дня введения их в действие. В случае если согласование по размеру комиссионного вознаграждения не будет достигнуто между Сторонами, Банк оставляет за собой право в одностороннем порядке отказаться от исполнения настоящего Договора, предварительно письменно уведомив об этом Клиента за 10 (десять) рабочих дней до даты расторжения Договора.

5.12. Банк вправе приостановить или прекратить предоставление услуг по Договору в случае невозможности взимания с Клиента комиссионного вознаграждения. Об этом Банк в письменной форме или электронным способом уведомляет Клиента в течение 10 (десять) рабочих дней со дня приостановления/прекращения предоставления услуг по Договору. В случае оплаты Клиентом услуг Банк вправе возобновить предоставление Клиенту услуг с уведомлением об этом Клиента в письменной форме или электронным способом.

Статья 6. Ответственность Сторон

6.1. За неисполнение или ненадлежащее исполнение обязательств по Договору Стороны несут ответственность в соответствии с условиями Договора и действующим законодательством.

6.2. Каждая Сторона не несет ответственности за убытки, понесенные другой Стороной не по вине первой в результате использования электронных документов, сообщений (указаний), в том числе при исполнении ошибочных электронных документов, сообщений (указаний), если эти документы, сообщения (указания) надлежащим образом оформлены, подтверждены и доставлены одной Стороной, а другой Стороной проверены и приняты.

6.3. Ответственность за своевременность и правильность совершения операций на основании электронных платежных документов, сообщений (указаний), Банк несет в соответствии с Договором.

6.4. Банк не несет ответственности за убытки, понесенные Клиентом в результате любых действий третьих лиц, включая, но не ограничиваясь контрагентами/работниками Клиента, которым по любым основаниям стали доступны Рабочая станция, Ключевой носитель, в случае подключения Системы с его использованием, Карт-ридер, в случае выбора Ключевого носителя – смарт-карты и Устройство eToken PASS, в случае выбора Клиентом данного Способа динамической аутентификации, информация о Pin-коде, если это стало возможным по неосторожности, небрежности и/или умыслу Клиента.

6.5. Банк не несет ответственности за исполнение/неисполнение/правильность исполнения электронных документов, сообщений (указаний) Клиента в случае, если Клиент несвоевременно уведомил/не уведомил Банк о прекращении или изменении объема полномочий лиц, указанных в заявлении на подключение пользователей, лиц, уполномоченных инициировать, подтверждать, направлять сообщения (указания) посредством Систем.

6.6. Вопросы возмещения убытков, включая реальный ущерб, упущенную выгоду, возникшие вследствие разглашения уполномоченным лицом Клиента Pin-кода, передачи независимо от причин третьим лицам, Ключевой носитель, в случае подключения Системы с его использованием, Карт-ридер, в случае выбора Ключевого носителя – смарт-карты и Устройство eToken PASS, в случае выбора Клиентом данного Способа аутентификации, разрешаются между Клиентом и уполномоченным лицом Клиента без участия Банка.

6.7. Клиент несет полную ответственность за корректное предоставление информации по Доверенному номеру, и в случае несанкционированного доступа к Мобильному устройству, которое используется для входа в Мобильное приложение и отправки Электронных документов, полностью несет ответственность за понесенные убытки.

Статья 7. Разрешение споров

7.1. Стороны принимают меры по урегулированию возникших споров, противоречий и разногласий путем переговоров и путем рассмотрения комиссией, создание которой предусмотрено данной статьей Договора.

7.2. При невозможности проведения переговоров либо невозможности разрешения споров, противоречий и разногласий путем переговоров они разрешаются в судебном порядке, установленном законодательством Республики Казахстан.

7.3. Все вопросы, прямо или косвенно связанные с Договором и не урегулированные в нем, решаются и регулируются Сторонами в соответствии с Договором, а во всем, что не урегулировано Договором – в соответствии с Действующим законодательством, а также внутренними нормативными документами Банка. Разрешение возникших между Сторонами споров, связанных с применением ЭЦП и/или Способа аутентификации осуществляется создаваемой для разрешения каждого конкретного спорного случая экспертно-технической комиссией.

7.4. Клиент представляет Банку заявление, содержащее существо претензии с указанием электронного документа, документа, на основании которого Банк выполнил операции по Счету. Банк обязан в течение не более 7 (семь) рабочих дней от даты подачи заявления Клиента сформировать экспертно-техническую комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента, Банка, удостоверяющего центра (если использовался электронный документ), представитель разработчика Системы (если сообщение (указание) было инициировано без использования Ключевого носителя) и при необходимости – представитель разработчика Системы, независимые эксперты. Экспертно-техническая комиссия правомочна рассматривать заявление Клиента при обязательном наличии в ее составе по одному представителю от Клиента, Банка и удостоверяющего центра/разработчика Системы.

7.5. Экспертно-техническая комиссия проводит рассмотрение заявления Клиента путем технической экспертизы открытого ключа ЭЦП Клиента и оспариваемого электронного документа, или сообщения (указания), инициированного без использования Ключевого носителя, включающей следующие этапы:

- установление времени проведения операции;
- проверка целостности программного обеспечения Системы, обеих Сторон путем вычисления контрольной суммы и ее сравнения с эталонной;
- осуществление проверки принадлежности закрытого ключа ЭЦП Клиенту/порядка предоставления Банком Клиенту доступа к услуге с использованием динамической идентификации Банком Клиента;
- осуществление проверки статуса регистрационного свидетельства соответствующему закрытому ключу Клиента и его срок действия в момент оформления документа/ работоспособности Устройства eToken PASS или другого, выбранного Клиентом, Способа аутентификации;
- проведение тестовой операции на сумму один тенге с использованием предъявленного Ключевого носителя для проверки работоспособности данного ключевого носителя. Из базы данных извлекаются данные по тестовой операции, по которым проверяется ЭЦП;
- проведение тестовой операции на сумму один тенге с использованием динамической идентификации Банком Клиента при инициировании Клиентом сообщения (указания) с помощью Способа аутентификации;
- извлечение данных и ЭЦП электронного документа из архива базы данных Системы и проверка подлинности ЭЦП Клиента/извлечение сообщения (указания) из архива базы данных Системы и проверка надлежащего порядка инициирования, подтверждения сообщения (указания).

На основании данных технической экспертизы составляется акт, который подписывается всем составом экспертно-технической комиссии.

7.6. В случае принятия Сторонами решения экспертно-технической комиссии оно должно быть выполнено не позднее следующего рабочего дня.

7.7. В случае отказа от исполнения решения экспертно-технической комиссии Стороны передают возникший между ними спор на рассмотрение в судебные органы в соответствии с действующим законодательством Республики Казахстан.

Статья 8. Форс-мажор

8.1. Если какой-либо из Сторон мешают или задерживают исполнение обязательств обстоятельства форс-мажора, которые описаны ниже, тогда исполнение Стороной обязательств

приостанавливается соразмерно времени, в течение которого длятся форс-мажорные обстоятельства, и в той степени, в какой они мешают или задерживают исполнение обязательств Стороной. Сторона, чье выполнение каких-либо обязательств в соответствии с Договором оказалось невозможным в силу наступления форс-мажорных обстоятельств, обязана в срок не позднее 3 (три) рабочих дней после наступления форс-мажорных обстоятельств уведомить об этом другую Сторону в письменной форме и предпринять все возможные действия для того, чтобы снизить потери или ущерб в отношении другой Стороны и восстановить свою способность выполнять обязательства по Договору.

8.2. Неуведомление или несвоевременное уведомление лишает Сторону права ссылаться на любое форс-мажорное обстоятельство как на основание, освобождающее от ответственности за неисполнение обязательств по Договору, за исключением случаев, когда такое неуведомление или несвоевременное уведомление прямо вызвано соответствующим форс-мажорным обстоятельством.

8.3. Форс-мажор означает любые обстоятельства непреодолимой силы, включая, но не ограничиваясь: пожары (за исключением происшедших вследствие преступной небрежности или халатности Сторон), наводнения, землетрясения, войны (объявленные и необъявленные), восстания, забастовки, гражданские войны или массовые беспорядки.

Статья 9. Действие Договора. Язык Договора

9.1. Договор вступает в силу с момента присоединения Клиента к условиям договора путем подписания заявления.

9.2. Договор действует бессрочно.

9.3. Договор расторгается:

9.3.1. в любое время по взаимному согласию Банка и Клиента;

9.3.2. считается расторгнутым в случае расторжения всех договоров и закрытия последнего из банковских счетов Клиента в Банке, открытых по таким договорам, по которым производились операции с использованием Систем, со дня закрытия последнего счета и расторжения последнего из договоров. В этом случае Стороны обязаны произвести взаиморасчеты по Договору не позднее 10 (десять) рабочих дней со дня расторжения Договора;

9.3.3. в случае отказа от Договора одной из Сторон, предупредившей (в виде письменного уведомления) об этом другую Сторону не позднее чем за 10 (десять) рабочих дней до даты расторжения Договора. При расторжении Договора Стороны обязаны исполнить друг перед другом все ранее возникшие и не прекратившие ко дню расторжения Договора обязательства по Договору и произвести взаиморасчеты не позднее даты расторжения, указанной в письменном уведомлении о расторжении. Отдельные случаи отказа Сторон от Договора могут предусматриваться в Условиях, не ограничивая при этом право каждой из Сторон отказаться от Договора в других случаях.

Статья 10. Заключительные положения

10.1. Клиент не вправе передавать или переводить любые права или обязательства в связи с Договором без предварительного письменного согласия Банка. Любые попытки такой передачи или перевода в нарушение настоящей статьи не имеют юридической силы и последствий.

10.2. Настоящий Договор представляет собой полное взаимопонимание Сторон и заменяет все предыдущие письменные или устные соглашения и договоренности, имевшиеся между ними в отношении оказания Клиенту электронных банковских услуг с использованием Системы.

10.3. Банк оставляет за собой право вносить изменения в одностороннем порядке, о чем информирует Клиента о таких изменениях (за исключением изменений в тарифах в перечне операций, предоставляемых при использовании Систем, порядок внесения которых регулируется иными нормами Договора) не менее чем за 10 (десять) рабочих дней до даты введения в действие решения уполномоченного органа Банка, внесшего изменения в Договор. Информирование производится посредством направления Клиенту письменного уведомления (подтверждение о получении такого уведомления Клиентом не требуется). После такого уведомления и в случае если Клиент не согласен с изменениями, Клиенту следует уведомить об этом Банк в письменной форме не позднее даты введения в действие изменений. В этом случае Клиент вправе отказаться от Договора без штрафных санкций, если штрафные санкции прямо не предусмотрены настоящим Договором. Возможные риски, связанные с неполучением Клиентом информации об изменениях в Договоре, возлагаются на Клиента.

В случае непредставления Клиентом возражений до указанной Банком даты введения в действие изменений в Договоре, Договор продолжает действовать с учетом изменений.

В случае, если Клиент до истечения, указанного в части первой настоящего пункта срока направит в Банк одним из способов, предусмотренных в настоящем пункте, письменное уведомление о согласии с изменениями в Договор, то такие изменения для Банка и Клиента будут считаться введенными в действие со дня получения Банком указанного письменного уведомления Клиента.

Письменное уведомление, направленное Банком в соответствии с настоящим пунктом, считается полученным Клиентом:

- 1) при отправке нарочным (курьером) – в день получения с соответствующей отметкой;
- 2) при отправке заказным письмом – на 4 (четвертый) календарный день после отправки (по дате документа, выданного почтовой организацией при отправке);
- 3) при отправке посредством Систем – в день отправки.

Письменное уведомление, направленное Клиентом в соответствии с настоящим пунктом, считается полученным Банком:

- 1) при отправке нарочным (курьером) – в день получения с соответствующей отметкой;
- 2) при отправке заказным письмом – на 4 (четвертый) календарный день после отправки (по дате документа, выданного почтовой организацией при отправке);
- 3) при отправке посредством Систем – в день отправки.

10.4. Любые издержки, понесенные Банком в случае вовлечения его в судебное разбирательство между Клиентом и третьими лицами, а также любые иные издержки Банка, которые могут возникнуть как следствие отношений Банка с Клиентом и которые не регулируются тарифами, относятся на счет Клиента. Банк предъявляет Клиенту к оплате счет с указанием суммы издержек. Клиент немедленно после получения указанного счета обязан его оплатить.

10.5. Все документы, имеющие отношение к настоящему Договору, должны составляться на государственном и/или русском языке, согласованном между Банком и Клиентом. Если Стороны договорятся составлять документы на двух языках, то в случае возможных разногласий относительно содержания таких документов Стороны руководствуются текстом соответствующего документа, составленного на русском языке.

Условия обслуживания через Систему «Onlinebank HALYK»

Статья 1. Подключение Системы

1.1. Клиент для подключения Системы должен заполнить Заявление по форме Приложений 1 и 2 к Условиям Onlinebank и предоставить все надлежащим образом оформленные документы в соответствии с требованиями Банка.

1.2. Клиент при заполнении Заявления на подключение Системы Onlinebank обязан выбрать Уровень безопасности.

1.3. Банк должным образом и доступными ему способами извещает о существовании версий Системы, таких как «Onlinebank HALYK Business» и «Onlinebank HALYK Start».

1.4. Подписывая заявление на подключение компании, согласно Приложению к Условиям Onlinebank, Клиент подтверждает, что Банк донес информацию о необходимых устройствах Ключевого носителя и/или Способе динамической аутентификации при подключении версий Системы «Onlinebank HALYK Business» или «Onlinebank HALYK Start».

1.5. Клиент не может быть подключен одновременно к двум имеющимся версиям Системы Onlinebank.

1.6. Клиент не может быть подключен к Мобильному приложению без подключения к Системе.

1.7. Мобильное приложение может быть подключено Клиенту только при указании Доверенного номера.

1.8. Подключение к Системе версией «Onlinebank HALYK Start» невозможно без указания Клиентом Доверенного номера.

1.9 Доверенный номер фиксируется в системах Банка и используется для направления одноразового (единовременного) кода в виде SMS-сообщения. Использование (ввод) Клиентом одноразового (единовременного) кода подтверждает идентификацию Клиента и является основанием для предоставления Клиенту доступа к Электронным банковским услугам.

При изменении номера мобильного (сотового) телефона Уполномоченного лица Клиента, зарегистрированного в системах Банка в качестве Доверенного номера, либо утери/кражи мобильного (сотового) телефона Клиент предоставляет в Банк Заявление на изменение/удаление Доверенного номера согласно приложению 3 к Условиям обслуживания через Систему «Onlinebank HALYK» Договора присоединения на регистрацию пользователя в Системе будет являться неотъемлемой частью Договора.

1.10. Клиент подтверждает, что при подписании Заявления, Банк уведомил Клиента о существовании в Банке различных Уровней безопасности при подключении Системы.

1.11. При выборе Уровня безопасности «Высокий» Клиент выбирает предложенное ему устройство Ключевого носителя (смарт-карту или устройство Java Token), а также один из Способов динамической аутентификации (Onlinebank-аутентификация, SMS аутентификация или аутентификация с помощью Устройства eToken PASS).

Клиент обязуется при первом входе в систему подключить доступный Способ динамической аутентификации и использовать данный Способ динамической аутентификации при отправке Электронных документов в Банк. В случае, если будет доказано, что Клиент не использовал, выбранный в Приложении 1 к Условиям Onlinebank, Способ динамической аутентификации, будет считаться, что Клиент подключил Систему с Уровнем безопасности «Средний», принимая все риски и не имеет никаких претензий к Банку в случае несанкционированного доступа к Системе.

1.12. При выборе Уровня безопасности «Средний» Клиент выбирает предложенное ему устройство Ключевого носителя (смарт-карту или устройство Java Token).

1.13. При выборе Уровня безопасности «Низкий» Клиент выбирает предложенный ему Способ динамической аутентификации (Onlinebank-аутентификация или SMS аутентификация).

1.14. Клиент подтверждает, что Банк, любыми выбранными им способами, донес информацию до Клиента о возникших рисках при подключении Системы Onlinebank и выборе Уровня безопасности отличным от «Высокий».

1.15. Клиент при выборе «Среднего» и «Низкого» Уровня безопасности полностью несет полную ответственность за возможность несанкционированного доступа к Рабочей станции,

возможные риски при отправке Электронных документов на исполнение в Банк, и в случае понесенного ущерба, включая реальный ущерб и/или упущенную выгоду, не имеет претензий к Банку.

1.16. Банк передает Клиенту выбранные Клиентом устройства при подключении в Системе, согласно Приложению 2 к Условиям Onlinebank, которые Клиент вправе использовать исключительно для получения электронных банковских услуг по Договору.

В случае, если Клиент при подключении Системы Onlinebank, выбрал Ключевой носитель – смарт-карту, Банк также передает Клиенту карт-ридер.

1.17. Гарантийный срок выданных Банком Устройств для аутентификации, составляет 1 год со дня выдачи работником Банка. В случае выхода из строя данного устройства в течение гарантийного срока по причине производственного брака замена осуществляется Банком бесплатно, при наличии видимых повреждений (по вине Клиента) – согласно тарифам Банка. В случае поломки устройства по истечении гарантийного срока замена производится на платной основе согласно тарифам Банка.

При отключении Клиента от Системы Onlienbank, поломке Устройств для аутентификации и/или истечении срока действия регистрационного свидетельства Клиента, все Устройства для аутентификации остаются у Клиента.

При утере Клиентом Устройств для аутентификации, Банк по инициативе Клиента повторно выдает Клиенту устройства на платной основе согласно тарифам Банка.

1.18. Стороны соглашаются, что Устройства для аутентификации, будут считаться переданными Банком Клиенту с момента подписания Сторонами акта приема-передачи по форме согласно Приложения 3 к Договору.

В случае, если акт приема-передачи по форме согласно Приложению 3 к Договору не был подписан Клиентом в течение 30 (тридцать) календарных дней с момента подписания Договора, то повторный перевыпуск ключей первичной инициализации должен происходить по инициативе Клиента на платной основе согласно тарифам Банка.

1.19. Физические лица, которые будут вправе подписывать Электронные документы Клиента в качестве уполномоченных лиц Клиента, будут определяться исходя из представленных Клиентом в Банк заявлений на подключение пользователя к Системе по форме согласно Приложению 2 к Условиям Onlinebank. Каждое представленное Клиентом заявление на регистрацию пользователя в Системе будет являться неотъемлемой частью Договора.

Статья 2. Оказание услуг в Системе

2.1. При оказании услуг в Системе Onlienabank обмен информацией между Клиентом и Банком осуществляется с использованием ЭЦП и/или Способом аутентификации.

2.2. Клиент должен заполнять документы, формировать сообщения (указания) в соответствии с действующим законодательством и инструкциями Банка, с которыми Банк предварительно знакомит Клиента, при этом вся ответственность, включая возможный причиненный ущерб за неправильное оформление документов, сообщений (указаний) возлагается на Клиента.

2.3. Информация на Ключевом носителе и/или информация по сгенерированном, одноразовом (единовременном) коде являются конфиденциальными. В случае, разглашения Клиентом данной информации третьим лицам, Банк не несет ответственность за понесенные ущербы, убытки Клиента.

2.4. Клиент имеет возможность использования Системы Onlinebank вне зависимости от времени и/или даты. В свою очередь, Электронные документы могут быть отправлены Клиентом в Банк для исполнения только в Операционный день.

Операционный день Банка устанавливается Банком и может быть изменен Банком в одностороннем порядке. Информацию о продолжительности операционного дня и/или его изменениях Банк доводит до сведения Клиента, любым доступным способом, в том числе, но не ограничивая себя, в операционных залах Банка.

2.5. Банк приостанавливает предоставление электронных банковских услуг по причине неисправности технических средств, обеспечивающих предоставление электронных банковских услуг, о чем Банк уведомляет Клиента. При устранении причин, повлекших приостановление предоставления электронных банковских услуг, Банк возобновляет предоставление Клиенту электронных банковских услуг по Договору с последующим уведомлением Клиента.

2.6. Для работы в Системе Клиент должен обеспечить самостоятельно наличие следующих программно-технических средств:

- компьютер не ниже следующей конфигурации: процессор – Celeron 1.6 ГГц, ОЗУ – от 1 Гб;
- операционная система Microsoft Windows 7 и выше, Mac OS последней версии, Linux;
- браузер Microsoft Internet Explorer не ниже 11 версии, Chrome, Mozilla, Opera последних версий;
- Java Runtime Environment (JRE) 8 и выше;
- криптопровайдер ONLINEBANK CSP;
- доступ в интернет на минимальной скорости от 2 Мб/с и выше;
- представитель Клиента должен иметь права администратора на своём компьютере;
- наличие антивирусного ПО с актуальными обновлёнными базами;
- наличие свободного USB-порта на компьютере Клиента.

При выборе Ключевого носителя Java Token:

- TUMAR-CSP последней версии (SafeNet).

При выборе Ключевого носителя на смарт-карте:

- Драйвер для карт-ридера;
- Панель управления KAZTOKEN (Kaztoken);
- в случае использования прокси-сервера для доступа к <https://halyk.onlinebank.kz> должен быть открыт порт 443 к 195.200.74.52 и 195.200.74.55.

2.7. Перечень операций, которые могут осуществляться посредством Системы с использованием электронных документов:

1) прием электронных платежных поручений на осуществление переводов в национальной валюте, в том числе:

- уплата налоговых платежей;
- перечисление обязательных пенсионных взносов, социальных отчислений, отчислений на обязательное медицинское страхование;
- осуществление платежей за товары и/или услуги;
- пополнение текущих счетов физических лиц;

2) прием электронных платежных поручений на осуществление переводов в иностранной валюте;

3) прием электронных заявок на конвертацию (покупка/продажа) иностранной валюты Клиентом;

4) прием электронных заявок на конвертацию посредством платформы «Halyk FX»;

5) предоставление Клиенту в электронном виде:

- финальной выписки о состоянии Счета;
- предварительной выписки;

6) прием от участников экспортно-импортного валютного контроля документов, связанных с валютным контролем (контракты, инвойсы, соглашения, счета на оплату, дополнительные соглашения и т.д.), за исключением дополнительных листов к паспортам сделок, паспортов сделок;

7) письма Сторон (запросы, заявки, уведомления и т.д.);

8) заявления на открытие сберегательного счета и внесение банковского вклада;

9) запросы на выпуск регистрационных свидетельств;

10) заявки-оферты на заключение договора гарантии (в рамках заключенного соглашения о предоставлении покрытых гарантий);

11) уведомления о поступлении/зачислении валюты;

12) любая другая банковская услуга или операция, которая может быть дополнительно внесена в данный перечень путем размещения информации на интернет-сайте Банка www.halykbank.kz. При появлении новых/прекращении предоставления ранее доступных с использованием Системы электронных услуг Банк в одностороннем порядке (без согласования с Клиентом) изменяет имеющийся на интернет-сайте www.halykbank.kz перечень операций, предоставляемых при использовании Системы, и публикует новый.

Допускается передача любой иной информации неплатежного характера, которая не входит в приведенный в настоящем пункте перечень, но эта информация не является основанием возникновения обязательств со стороны Банка.

2.8. Перечень условий по конвертациям, проходящим через платформу «Halyk FX»:

1) Заявка на конвертацию, отправленная через платформу «Halyk FX» подтверждается клиентом в момент сохранения/ подтверждения заявки и распознается Банком, как согласованный с Казначейством Банка;

2) При заведении одним клиентом 2 заявок на конвертацию с одинаковой суммой, валютой и стороной сделки, платформа не позволяет завести 3-ю заявку с аналогичными 2-м предшествующим заявкам условиям;

3) При заведении одним клиентом нескольких заявок на конвертацию, но не подписанными и не отправленными в Банк по истечению текущего операционного дня, на систематических условиях, Банк вправе отключить платформу «Halyk FX» у данного клиента.

2.9. Электронный документ порождает обязательства Сторон в соответствии с настоящим Договором, если надлежащим образом оформлен, заверен ЭЦП и/или подтвержден одним из Способов аутентификации, доставлен по указанной в настоящем Договоре системе телекоммуникаций передающей Стороной, а принимающей Стороной проверен и принят.

2.10. Банк не принимает Электронные документы и сообщения (указания) к обработке в следующих случаях:

- если документ не подписан;
- если документ не зашифрован;
- если документ зашифрован не для принимающей Стороны;
- если документ искажен после постановки подписи;
- если регистрационное свидетельство подписавшего документ имеет статус «отозвано»;
- если срок действия регистрационного свидетельства владельца истек.

2.11. Документ, сообщение не будет обработан Банком в случаях:

- если дата валютирования указана более ранняя, чем дата фактической отправки документа;
- недостаточности денег на Счете;
- наличия к счету требований третьих лиц (картотека 2);
- наложения на Счет ареста Уполномоченными органами;
- отправки платежного документа во фродо-опасные страны;
- некорректного заполнения Электронного документа;
- иные случаи, предусмотренные внутренними нормативными документами Банка и/или Действующим законодательством.

2.12. Стороны взаимно обязуются принимать на себя в полном объеме все обязательства, вытекающие из электронных документов, подписанных их закрытыми ключами ЭЦП, регистрационные свидетельства, которые зарегистрированы в удостоверяющем центре, если проверка ЭЦП прошла успешно и к моменту приема документа не было зафиксировано официального заявления, подписавшего документ лица о компрометации своего закрытого ключа ЭЦП или программного обеспечения. Невыполнение любой из Сторон этого условия является основанием для отказа от Договора другой Стороной.

2.13. Клиент признает, что закрытые ключи ЭЦП, полученные путем смены ключей первичной инициализации, находятся на ключевом носителе и выпущены в единственном экземпляре.

2.14. Банк хранит электронные документы в том формате, в котором они были сформированы, отправлены или получены с соблюдением их целостности и неизменности с даты подключения Клиента к Системе, но не более 1 года. Банк не осуществляет распечатку электронных документов на бумажном носителе с целью их хранения или передачи Клиенту.

Банк осуществляет распечатку электронных документов на бумажном носителе по запросу Клиента, за каждый экземпляр которого Банк взимает комиссионное вознаграждение в соответствии с действующими тарифами.

2.15. Клиент в качестве дополнительной опции дистанционного управления Счетом в рамках электронных банковских услуг может использовать Мобильное приложение, которое Клиент может подключить самостоятельно через настройки в Системе версией «Onlinebank HALYK Business» или автоматически при подключении Системы версией «Onlinebank HALYK Start».

2.16. При получении доступа к Системе Onlinebank посредством Мобильного приложения, Клиент должен обеспечить самостоятельное наличие мобильного устройства, отвечающего следующим параметрам:

- версия мобильной ОС не ниже Android 4.X и iOS 10.0;
- с минимальным размером экрана не меньше 800 x 480 (hdpi) для устройств на базе мобильной ОС Android.

2.17. Клиент признает, что Мобильное приложение является неотъемлемой частью Системы и невозможно без подключения к Системе.

2.18. В случае, если Клиент не обратился в Банк для получения Ключевых носителей и/или за устройством необходимых для Способа динамического аутентификации в течение 45 календарных дней после подачи полного пакета документа на подключение Системы Onlinebank, Банк не выдает Ключевые носители и/или за устройством необходимых для выбранного Способа динамического аутентификации взимает комиссию за подключение системы в соответствии с тарифами Банка.

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ КЛИЕНТА К СИСТЕМЕ И ПРИСОЕДИНЕНИЕ К ДОГОВОРУ

Полное наименование Клиента:

БИН/ИИН:

Настоящим Клиент подтверждает, что:

1. ознакомился со всеми условиями Договора присоединения (далее – Договор), размещенного на официальном сайте Банка www.halykbank.kz, и понимает их текст, выражает свое согласие с ними и обязуется их выполнять надлежащим образом и принимает их в полном объеме путем присоединения к предложенному Договору в целом и дает согласие Банку на изменение и дополнение Договора в порядке, установленном в Договоре.
2. осведомлен о возможности заключения с Банком сделки по подключению к системе «Onlinebank HALYK» обычным способом, но делает выбор в пользу заключения Договора путем присоединения.

Настоящим подтверждает наличие программно-технических средств, указанных в п. 2.6 Условий Onlinebank, и просит предоставить доступ к системе «Onlinebank HALYK»

Контактный мобильный номер Клиента¹:

+7

Выбор версии и Профиля безопасности

☐ **Высокий**

Выберите Ключевой носитель:

- ☐ Java Token
☐ Смарт-карта

Выберите Способ динамической аутентификации:

- ☐ Устройство eTokenPass
☐ Online аутентификатор

☐ **Средний**

Доступна работа только через Смарт-карту

Дополнительно, Клиент может самостоятельно подключить услугу SMS-аутентификации*

☐ **Низкий**

Только для Onlinebank Start.

Работа без ключевого носителя со следующим способом динамической аутентификации - SMS аутентификация*

При выборе данного Профиля безопасности Банком могут быть выставлены лимиты. Подробнее на официальной странице Банка: www.halykbank.kz
Выбирая данный Профиль безопасности Клиент подтверждает, что осведомлен об имеющихся лимитах в Системе на совершение операций.

*За подключение SMS-аутентификации взимается ежемесячная дополнительная комиссия согласно тарифам Банка

☐ Для удалённого доступа ко всем счетам организации

☐ Для удалённого доступа к нижеперечисленным счетам:

№	Номер счета	Валюта счета
1		
2		
3		
4		
5		
6		

Фамилия, имя, отчество (при его наличии)
руководителя

Принято Банком

М.П.
(при наличии)

Подпись _____

« ____ » _____ года

Фамилия, имя, отчество (при его наличии)
главного бухгалтера

Подписи ответственных исполнителей Банка

Подпись _____

штамп

¹ Указывается мобильный номер Клиента, на который придет SMS о готовности Ключевых носителей

Приложение 2
к Условиям обслуживания
через Систему «Onlinebank HALYK»

**ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ К СИСТЕМЕ
БИН/ИИН:**

Полное наименование Клиента:

БИН/ИИН:

I. Просим предоставить доступ к Системе для пользователя (-ей):

Наименование поля	Уполномоченный работник №__	Уполномоченный работник №__ (при отсутствии работника проставить в ФИО – «отсутствует»)
Ф.И.О. уполномоченного работника		
Должность		
Документ, удостоверяющий личность	вид документа: _____ номер: _____ серия: _____ дата выдачи: «__» _____ 20__ г. орган, выдавший документ: _____ срок действия: «__» _____ 20__ г. ИИН: _____	вид документа: _____ номер: _____ серия: _____ дата выдачи: «__» _____ 20__ г. орган, выдавший документ: _____ срок действия: «__» _____ 20__ г. ИИН: _____
Контактные данные	Телефон: _____ Email: _____ Доверенный номер ² _____	Телефон: _____ Email: _____ Доверенный номер _____
Лимит на сумму одной операции в тенге		
Право подписи	☐ единственная подпись ☐ без права подписи ☐ право расширенной подписи ☐ право _____ подписи ³	☐ единственная подпись ☐ без права подписи ☐ право расширенной подписи ☐ право _____ подписи
Область использования регистрационного свидетельства: первичная инициализация. Срок действия регистрационного свидетельства первичной инициализации – 30 дней.		

Необходим карт ридер в количестве _____ шт.

Печать при наличии	Фамилия, имя, отчество (при его наличии) руководителя Подпись _____	Принято Банком «__» _____ года Подписи ответственных исполнителей Банка М.П.
	Фамилия, имя, отчество (при его наличии) главного бухгалтера Подпись _____	

² Для подключения OnlineBank START обязательно поле для заполнения «Доверенный номер». Будет использоваться для SMS-аутентификации и SMS-информирования.

³ Возможно указание от 1 до 10 уровней подписания документов.

ЗАЯВЛЕНИЕ НА ИЗМЕНЕНИЕ/УДАЛЕНИЕ ДОВЕРЕННОГО (МОБИЛЬНОГО) НОМЕРА

Полное наименование Клиента:

БИН/ИИН:

Контактный телефон Клиента: _____

E-mail Клиента: _____

Прошу Вас Доверенный (мобильный) номер

- ☐ Удалить
☐ Изменить

С действующего:

+7										
----	--	--	--	--	--	--	--	--	--	--

На (заполняется в случае «Изменения номера»:

+7										
----	--	--	--	--	--	--	--	--	--	--

М.П.
(при наличии)

Фамилия, имя, отчество (при его наличии)
руководителя

Подпись _____

Фамилия, имя, отчество (при его наличии)
главного бухгалтера

Подпись _____

Принято Банком

« ____ » _____ года

Подписи ответственных исполнителей Банка

штамп

Условия обслуживания через Систему «Correqts»

Статья 1. Подключение Системы

1.1. При оказании услуг в Системе Correqts обмен информацией между Клиентом и Банком осуществляется с использованием ЭЦП и/или посредством МБК.

1.2. Клиент для работы в Системе Correqts должен заполнить Заявление по форме Приложения к настоящему Условиям Correqts и предоставить все надлежащим образом оформленные документы в соответствии с требованиями Банка.

1.3. Клиент должен заполнять документы, формировать сообщения (указания) в соответствии с действующим законодательством и инструкциями Банка, с которыми Банк предварительно знакомит Клиента, при этом вся ответственность, включая возможный причиненный ущерб за неправильное оформление документов, сообщений (указаний) возлагается на Клиент

1.4. Информация на ключевом носителе и пароль доступа являются конфиденциальными.

1.5. Стороны соглашаются, что ключи первичной инициализации, устройство eToken PASS и ключевой носитель будут считаться переданными Банком Клиенту с момента подписания Сторонами акта приема-передачи по форме согласно Приложению 3 к Договору.

В случае, если акт приема-передачи по форме согласно Приложению 3 к Договору не был подписан Клиентом в течение 30 (тридцать) календарных дней с момента подписания Договора, то повторный перевыпуск ключей первичной инициализации должен происходить по инициативе Клиента на платной основе согласно тарифам Банка.

1.6. Банк передает Клиенту устройство eToken PASS и ключевой носитель, которые Клиент вправе использовать исключительно для получения электронных банковских услуг по Договору.

Гарантийный срок ключевого носителя и устройства eToken PASS составляет 1 год со дня выдачи работником Банка. В случае выхода из строя данного устройства в течение гарантийного срока по причине производственного брака замена осуществляется Банком бесплатно, при наличии видимых повреждений (по вине Клиента) – согласно тарифам Банка. В случае поломки устройства по истечении гарантийного срока замена производится на платной основе согласно тарифам Банка.

При отключении Клиента от Системы Correqts, поломке ключевого носителя или устройства eToken PASS, истечении срока действия регистрационного свидетельства Клиента ключевой носитель и устройство eToken PASS остаются у Клиента.

При утере Клиентом устройства eToken PASS или ключевого носителя Банк по инициативе Клиента повторно выдает Клиенту устройство eToken PASS или ключевой носитель на платной основе согласно тарифам Банка.

1.7. Операционный день Банка устанавливается Банком и может быть изменен Банком в одностороннем порядке. Информация о продолжительности операционного дня и/или его изменениях размещается в операционных залах Банка. Если электронные документы, сообщения (указания), документы Клиента в МБК получены Банком:

- до окончания операционного дня, они проводятся тем же операционным днем;
- после окончания операционного дня, они проводятся следующим операционным днем (при наличии технической возможности у Банка – тем же операционным днем).

1.8. Если по какой-либо причине одна Сторона не может своевременно доставить документы другой Стороне посредством Системы Correqts, то эта Сторона должна предпринять меры по доставке соответствующим образом оформленных платежных документов на бумажном носителе.

Банк приостанавливает предоставление электронных банковских услуг по причине неисправности технических средств, обеспечивающих предоставление электронных банковских услуг, о чем Банк уведомляет Клиента. При устранении причин, повлекших приостановление предоставления электронных банковских услуг, Банк возобновляет предоставление Клиенту электронных банковских услуг по Договору с последующим уведомлением Клиента.

Статья 2. Оказание услуг в Системе

2.1. Для работы в Системе Correqts Клиент должен обеспечить самостоятельно наличие следующих программно-технических средств:

Гб;

- компьютер не ниже следующей конфигурации: процессор – Celeron 1.6 ГГц, ОЗУ – от 1
- операционная система Microsoft Windows 7 и выше;
- браузеры Microsoft Internet Explorer 11.0, Chrome, Mozilla, Opera или более новые версии;
- доступ в интернет на минимальной скорости от 2 Мб/с и выше;
- в случае использования прокси-сервера для доступа к <https://ib.halykbank.kz> должен быть открыт порт 443 к 195.200.74.70 и порт 1024 к 195.200.74.80, для <https://online.halykbank.kz/> должен быть открыт порт 443 к 195.200.74.61;

- Microsoft Word 2003, Excel 2003 и выше, Acrobat reader;
- наличие подключенного сетевого или локального принтера;
- представитель Клиента должен иметь права администратора на своём компьютере;
- наличие антивирусного ПО с актуальными обновлёнными базами;
- наличие свободного USB-порта на компьютере Клиента.

2.2. Перечень операций, которые могут осуществляться посредством Системы с использованием электронных документов:

1) прием электронных платежных поручений на осуществление переводов в национальной валюте, в том числе:

- уплата налоговых платежей;
- перечисление обязательных пенсионных взносов и социальных отчислений;
- оплата услуг провайдеров сотовой связи;
- осуществление платежей за товары и/или услуги;
- пополнение текущих счетов физических лиц;

2) прием электронных платежных поручений на осуществление переводов в иностранной валюте;

3) прием электронных заявок на конвертацию (покупка/продажа) иностранной валюты Клиентом;

4) предоставление Клиенту в электронном виде:

- финальной выписки о состоянии Счета;
- предварительной выписки (Справка по Счету);
- выписки по POS-терминалам (при наличии);
- выписки по текущим счетам в карточной базе;

5) предоставление информации по справочникам (контрагентов, кодов назначения платежа, кодов бюджетной классификации, банков и т.д.);

6) прием от участников экспортно-импортного валютного контроля документов, связанных с валютным контролем (контракты, инвойсы, соглашения, счета на оплату, дополнительные соглашения и т.д.), за исключением дополнительных листов к паспортам сделок, паспортов сделок;

7) письма Сторон (запросы, заявки, уведомления и т.д.);

8) заявления на открытие сберегательного счета и внесение банковского вклада;

9) заявление на закрытие текущего банковского счета;

10) запросы на выпуск регистрационных свидетельств;

11) заявки-оферты на заключение договора гарантии (в рамках заключенного соглашения о предоставлении покрытых гарантий);

12) уведомления о поступлении/зачислении валюты;

13) заявления на досрочное погашение банковского займа;

14) заявления на выпуск/перевыпуск корпоративной платежной карточки, а также любого документа, который может быть дополнительно внесен в данный перечень путем размещения информации на интернет-сайте Банка www.halykbank.kz. При появлении новых/прекращении предоставления ранее доступных с использованием Системы электронных услуг Банк в одностороннем порядке (без согласования с Клиентом) изменяет имеющийся на интернет-сайте www.halykbank.kz перечень операций, предоставляемых при использовании Системы, и публикует новый.

Допускается передача любой иной информации неплатежного характера, которая не входит в приведенный в настоящем пункте перечень, но эта информация не является основанием возникновения обязательств со стороны Банка.

2.3. Банк передает Клиенту неисключительную лицензию на использование программы обработки и хранения информации «ДБО BS Client» для работы в Системе Correqts без права

передачи. Клиент обязуется не изменять, не проводить анализ, не копировать, не публиковать и не передавать копии такой программы и не содействовать любой третьей стороне в использовании и копировании Системы.

В момент передачи программного обеспечения Банк передает Клиенту в пределах срока охраны имущественных прав, предусмотренного в законодательстве Республики Казахстан об авторском праве, на все время действия Договора следующее имущественное право на программное обеспечение – право на использование.

В соответствии с Договором Банк передает Клиенту имущественное право на использование программного обеспечения на территории Республики Казахстан.

2.4. Физические лица, которые будут вправе подписывать своей ЭЦП электронные документы Клиента в качестве уполномоченных лиц Клиента, будут определяться исходя из представленных Клиентом в Банк заявлений на регистрацию пользователя в Системе по форме согласно Приложения к Условиям Correqts. Каждое представленное Клиентом заявление на регистрацию пользователя в Системе будет являться неотъемлемой частью Договора.

2.5. Электронный документ порождает обязательства Сторон в соответствии с настоящим Договором, если надлежащим образом оформлен, заверен ЭЦП, доставлен по указанной в настоящем Договоре системе телекоммуникаций передающей Стороной, а принимающей Стороной проверен и принят.

2.6. После получения электронного документа принимающая Сторона должна своевременно передать обратно электронную квитанцию, уведомляющую о принятии или отказе в принятии электронного документа.

2.7. Квитанция о приеме электронного документа означает окончательное подтверждение, что документ получен.

2.8. Документы со следующими ошибками принимают статус «ЭЦП неверна»:

- документ не подписан;
- документ не зашифрован;
- документ зашифрован не для принимающей Стороны;
- документ искажен после постановки подписи;
- регистрационное свидетельство подписавшего документ имеет статус «отозвано»;
- срок действия регистрационного свидетельства владельца истек.

2.9. Документ не будет обработан также в случаях:

- если дата валютирования указана более ранняя, чем дата фактической отправки документа;
- недостаточности денег на Счете;
- наличия к счету требований третьих лиц (картотека 2);
- наложения на Счет ареста Уполномоченными органами;
- отправки платежного документа во фродо-опасные страны.

2.10. В случае, когда при обработке электронного документа система обработки выдаст сообщение об одной из причин, указанных в пунктах 2.8. и 2.9 настоящих Условий, принимающая Сторона обязана не принимать к исполнению полученный электронный документ.

2.11. Стороны должны уведомлять друг друга о фактах неполучения квитанции на переданный электронный документ в день его отправки.

2.12. Стороны взаимно обязуются принимать на себя в полном объеме все обязательства, вытекающие из электронных документов, подписанных их закрытыми ключами ЭЦП, регистрационные свидетельства, которые зарегистрированы в удостоверяющем центре, если проверка ЭЦП прошла успешно и к моменту приема документа не было зафиксировано официального заявления, подписавшего документ лица о компрометации своего закрытого ключа ЭЦП или программного обеспечения. Невыполнение любой из Сторон этого условия является основанием для отказа от Договора другой Стороной.

2.13. Клиент признает, что закрытые ключи ЭЦП, полученные путем смены ключей первичной инициализации, находятся на ключевом носителе и выпущены в единственном экземпляре.

2.14. Банк хранит электронные документы в том формате, в котором они были сформированы, отправлены или получены с соблюдением их целостности и неизменности с даты подключения Клиента к Системе Correqts, но не более 1 года. Банк не осуществляет распечатку электронных документов на бумажном носителе с целью их хранения или передачи Клиенту.

Банк осуществляет распечатку электронных документов на бумажном носителе по запросу Клиента, за каждый экземпляр которого Банк взимает комиссионное вознаграждение в соответствии с действующими тарифами.

2.15. Клиент имеет возможность использования Системы Correqts вне зависимости от времени и/или даты. В свою очередь, Электронные документы могут быть отправлены Клиентом в Банк для исполнения только в Операционный день.

Операционный день Банка устанавливается Банком и может быть изменен Банком в одностороннем порядке. Информацию о продолжительности операционного дня и/или его изменениях Банк доводит до сведения Клиента, любым доступным способом, в том числе, но не ограничивая себя, в операционных залах Банка.

2.16. Банк приостанавливает предоставление электронных банковских услуг по причине неисправности технических средств, обеспечивающих предоставление электронных банковских услуг, о чем Банк уведомляет Клиента. При устранении причин, повлекших приостановление предоставления электронных банковских услуг, Банк возобновляет предоставление Клиенту электронных банковских услуг по Договору с последующим уведомлением Клиента.

2.17. В случае если Клиент не обратился в Банк для получения Ключевых носителей и/или за устройством необходимых для выбранного Способа динамической аутентификации в течение 45 календарных дней после подачи полного пакета документа на подключение Системы Correqts, Банк не выдает Ключевые носители и/или за устройством необходимых для Способа динамической аутентификации взимает комиссию за подключение системы в соответствии с тарифами Банка.

Статья 3. Оказание услуг с использованием Клиентом МБК

3.1. Клиент в качестве дополнительной опции дистанционного управления Счетом в рамках электронных банковских услуг может использовать услугу МБК, предоставляемую Банком на основании соответствующего Заявления Клиента.

При получении доступа к Системе Correqts посредством МБК или для получения услуги МБК без подключения к Системе Correqts Клиент должен обеспечить самостоятельное наличие мобильного устройства, отвечающего следующим параметрам:

- версия мобильной ОС не ниже Android 4.X и iOS 8.0;
- с минимальным размером экрана не меньше 800 x 480 (hdpi) для устройств на базе мобильной ОС Android.

3.2. В случае если доступ к Системе Correqts получен посредством МБК, то Клиенту доступен следующий перечень функций через МП:

- 1) создание сообщений (указаний) в виде платежных поручений для осуществления переводов в национальной валюте, их подтверждение и отправка в Банк на исполнение;
- 2) предоставление Клиенту информации в виде выписок по Счету и деталей операций;
- 3) справочники, содержащие:
 - информацию об отделениях и банкоматах Банка;
 - уведомления от Банка для Клиентов;
 - информацию о курсах валют;
- 4) подтверждение Банку о необходимости исполнения Банком платежных документов Клиента в тенге в МБК, инициированных из Системы;
- 5) информация о платежных поручениях, не прошедших оплату со статусом «отказано»;
- 6) отзыв платежного документа, до момента присвоения ему статуса «исполнен»;
- 7) письма Сторон (запросы, заявки, уведомления и т.д.).

3.3. Отправка платежного документа, созданного напрямую через МП, возможна лишь в пределах установленного Банком лимита на совершение операций в течение одного рабочего дня.

Размер лимита устанавливается и настраивается на стороне Банка. Данный лимит не распространяется на сообщения (указания) о платеже, инициированные и подтвержденные Клиентом непосредственно в Системе. Но в этом случае такие сообщения (указания) имеют ограничение на редактирование через МБК.

3.4. Сообщения (указания), инициированные Клиентом из МБК, подтверждаются Клиентом с использованием устройства eToken PASS. Необходимость проверки и проставления ЭЦП на такие сообщения (указания) не распространяется.

3.5. Клиент принимает на себя все обязательства, связанные с созданием и подтверждением инициированного им сообщения (указания) в МБК.

Приложение
к Условиям обслуживания
через Систему «Correqts»

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ КЛИЕНТА К СИСТЕМЕ И ПРИСОЕДИНЕНИЕ К ДОГОВОРУ

Полное наименование Клиента: _____

БИН/ИИН: _____

Настоящим Клиент подтверждает, что:

1. ознакомился со всеми условиями Договора присоединения (далее – Договор) и Условиям Correqts, размещенного на официальном сайте Банка www.halykbank.kz, и понимает их текст, выражает свое согласие с ними и обязуется их выполнять надлежащим образом и принимает их в полном объеме путем присоединения к предложенному Договору в целом и дает согласие Банку на изменение и дополнение Договора в порядке, установленном в Договоре.

2. осведомлен о возможности заключения с Банком сделки по подключению к системе «Интернет-банкинг для юридических лиц» обычным способом, но делает выбор в пользу заключения Договора путем присоединения.

Настоящим подтверждает наличие программно-технических средств, указанных в п.2.1 и/или п.3.1 Условий Correqts, и просит предоставить доступ к системе «Интернет-банкинг для юридических лиц» Correqts посредством модуля «Интернет-Клиент» и/или посредством МБК:

I. Подключение клиента к системе⁴:

☐ Доступ только через модуль «Интернет-клиент»

☐ Доступ через модуль «Интернет-клиент» и МБК

☐ Доступ только через МБК

☐ Доступ через модуль «Банк-партнер»

для удалённого доступа к следующим счетам:

№	Номер счета	Валюта счета
1		
2		
3		

II. Подключение пользователей к системе:

Просим предоставить доступ к Системе для пользователя, подключающегося через МБК, и/или ключи и регистрационное свидетельство первичной инициализации для пользователя, подключающегося к модулю «Интернет-клиент»:

Наименование поля	Уполномоченный работник №1	Уполномоченный работник №2 (при отсутствии работника проставить в ФИО – «отсутствует»)
Ф.И.О. уполномоченного работника		
Наименование места работы, должность		
Документ, удостоверяющий личность	вид документа: _____ номер: _____ серия: _____ дата выдачи: «___» _____ 20__ г. орган, выдавший документ: _____ срок действия: «___» _____ 20__ г. ИИН: _____	вид документа: _____ номер: _____ серия: _____ дата выдачи: «___» _____ 20__ г. орган, выдавший документ: _____ срок действия: «___» _____ 20__ г. ИИН: _____
Контактные данные	Телефон: _____ Email: _____	Телефон: _____ Email: _____
Лимит на сумму одной операции в тенге (при наличии)		
Право подписи	☐ единственная подпись ☐ право любой подписи ☐ без права подписи ☐ право расширенной подписи ☐ право _____ подписи ⁵	☐ единственная подпись ☐ право любой подписи ☐ без права подписи ☐ право расширенной подписи ☐ право _____ подписи ⁵

Область использования регистрационного свидетельства: первичная инициализация

Срок действия регистрационного свидетельства первичной инициализации – 30 дней.

Ф.И.О. _____

Должность _____

Подпись _____

М.П.

Дата: ____ / ____ / ____
 день месяц год

Время: ____ / ____
 часы минут

⁴ Заполняется только при первичном подключении клиента к Системе.

⁵ Возможно указание от 1 до 10 уровней подписания документов.

Приложение 3
к Договору присоединения
на обслуживание в системах дистанционного банковского
обслуживания

АКТ ПРИЕМА-ПЕРЕДАЧИ

г. _____

« ____ » _____ 20 ____ г.

Мы, нижеподписавшиеся, подтверждаем передачу Устройств указанных в заявлении на подключение клиента к системе Onlinebank HALYK версией Business или системе Coreqts (далее – Система), согласно Приложению к Условиям Onlinebank или Приложению к Условиям Coreqts (далее – Приложение).

Ключевой носитель _____ шт.

Карт-ридер _____ шт.

Устройство eToken PASS _____ шт.

_____.

(Ф.И.О. держателя ключа, наименование организации)

Передал:

Работник Банка, передавший Устройства, выбранные Клиентом для подключения к Системе, согласно Приложению и регистрационное свидетельство первичной инициализации.

(Ф.И.О.)

(подпись)

(должность)

(Ф.И.О.)

(подпись)

(должность)

Принял:

Уполномоченное лицо Клиента, получившее Устройства, выбранные Клиентом для подключения к Системе, согласно Приложению и регистрационное свидетельство первичной инициализации
(доверенность № _____ от « ____ » _____ 20 ____ г.)

(Ф.И.О.)

(подпись)

(должность)

Дата, время передачи: « ____ » _____ 20 ____ г. _____

(час, мин.)

Уполномоченный представитель Клиента:

(Ф.И.О. уполномоченного представителя Клиента)

Подпись _____

М.П.

Приложение 4
к Договору присоединения
на обслуживание в системах дистанционного банковского
обслуживания

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ К/ОТ УСЛУГЕ(-И) «SMS-УВЕДОМЛЕНИЕ»

Настоящим _____ в лице _____, действующего на основании _____, просит подключить к услуге/отключить от услуги «SMS-уведомление» /изменить номер следующих лиц:
(нужное подчеркнуть или обвести)

№	Ф.И.О. работника	Должность	Номер мобильного телефона
1			
2			
3			
4			
5			

Клиент: _____
(наименование клиента)

Ф.И.О. _____
(уполномоченного лица со стороны Клиента)

Должность _____
(уполномоченного лица со стороны Клиента)

Подпись _____
М.П.

Дата: ____ / ____ / ____

день месяц год

Время: ____ / ____

часы минуты