Договор присоединения

на обслуживание в системе «Onlinebank HALYK»

(с учетом изменений и дополнений, ПЗЗП от 08 апреля 2021 года № 336)

Настоящий Договор присоединения на обслуживание в системе «Onlinebank HALYK» (далее – Договор) регулирует отношения между Клиентом и АО «Народный Банк Казахстана», далее совместно именуемыми «Стороны», а по отдельности «Сторона». Условия настоящего Договора определены в стандартной форме.

Клиент присоединяется к Договору путем проставления своей подписи в Заявлении по форме Приложения 1 к настоящему Договору. При этом Заявление по форме Приложения 1 к настоящему Договору и Договор рассматриваются только в качестве единого документа. Присоединиться к Договору Клиент может при регистрации в системе «Onlinebank HALYK» (далее – Система Onlinebank) с использованием одноразового пароля.

Подпись Клиента, его представителя(-ей) на Заявлении (либо подтверждение одноразовым паролем) 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. Договор считается заключенным и вступает в силу со дня приема Банком Заявления (либо подтверждения одноразовым паролем) Клиента, подписанного Клиентом/его представителем.

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 Системе Onlinebank, оказания электронных банковских услуг Клиенту, совершения Клиентом операций по банковским счетам посредством Системы Onlinebank, и предоставления Банком иных услуг с использованием Системы Onlinebank, предусмотренных в настоящем Договоре.

Статья 1. Предмет Договора

1.1. Предметом Договора является предоставление Банком электронных банковских услуг и иных услуг, предусмотренных в Договоре, посредством Системы Onlinebank, при условии оплаты Клиентом данных услуг на условиях Банка.

При оказании Банком Клиенту вышеуказанных услуг, обслуживание Банком Клиента осуществляется согласно условиям настоящего Договора и условиям соответствующего договора банковского обслуживания.

1.2. Стороны признают, что документы в электронной форме (далее – электронные документы), используемые при совершении операций в Системе Onlinebank и/или посредством Мобильного приложения, подписанные электронной цифровой подписью (далее – ЭЦП) и/или одним из Способов 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 регистрационного свидетельства, прошедшего 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 ЭЦП и/или Способа динамической аутентификации.

1.6. Клиент признает, что при подписании Заявления на подключение к системе «Onlinebank HALYK» (либо подтверждении одноразовым паролем) он соглашается с Договором.

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.

Cash by code	Услуга Банка по выдаче Клиенту наличных денег с текущего счета через банкомат по сгенерированному коду.
«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 Limit»	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, а также проведения Электронных документов в пользу контрагентов только при предоставлении оригинала Электронных документов.
«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 на сайте www.halykbank.kz Увеличение лимита может быть рассмотрено Банком при оплате Клиентом данной услуги по Тарифам Банка, указанным на сайте www.halykbank.kz
Onlinebank-аутентификатор	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.
OTP-пароль (One Time Password, одноразовый пароль)	Уникальная последовательность электронных цифровых символов, высылаемая Банком на доверенный номер Заявителя и предназначенная для одноразового использования при предоставлении доступа Клиенту к Электронным банковским услугам - Аутентификации. OTP-пароль предназначен для проведения Аутентификации Клиента для установления его подлинности с целью однозначного подтверждения его прав на получение Электронных банковских услуг и равнозначен его подписи.
Pin-код	Секретный код, известный только владельцу сертификата (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-сообщения 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 Onlinebank и/или авторизации платежей требуется создание и использование нового одноразового (единовременного) кода. На SMS-аутентификацию платежей Банк может установить суточный лимит. Информация по лимитам размещена на сайте www.halykbank.kz
SMS-информирование	Услуга, предоставляемая Банком для информирования Клиента об операциях по текущим счетам путем отправки SMS-сообщений Банком на Доверенный номер Клиента и подключаемая Клиентом самостоятельно в Системе Onlinebank. Размер комиссионного вознаграждения за подключение к Услуге определяется согласно Тарифам Банка на сайте www.halykbank.kz
Автокасса (АК)	Устройство для осуществления операций по приему/выдаче наличных денег на/с текущий (-его) счета по сгенерированному штрих-коду в Системе Onlinebank.
Банк	АО «Народный Банк Казахстана», включая его филиалы.
Верификация мобильного устройства	Процедура подтверждения мобильного устройства Клиента с целью реализации им прав и исполнения обязательств по Договору. При верификации устройства присваивается токен для мобильного устройства, далее авторизация в Мобильном приложении осуществляется

	путем ввода Клиентом Pin -кода и/ или при помощи средств биометрической аутентификации.
Владелец регистрационного свидетельства	Физическое лицо, являющееся уполномоченным представителем юридического лица на основе Заявления на подключение пользователя к Системе Onlinebank, на имя которого Удостоверяющим центром выдан сертификат, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в сертификате, которому выпускаются ключ, и/или сертификат Облачной ЭЦП в защищенной области аппаратного модуля системы безопасности HSM.
Выписка	Надлежащим образом оформленный документ (на бумажном носителе или в электронной форме) о состоянии Счета Клиента за определенный период времени. В Системе Onlinebank предусмотрены два типа выписок по счёту: предварительная за текущий операционный день и финальная за закрытый операционный день.
Действующее законодательство	Законодательство Республики Казахстан, состоящее из нормативных правовых актов, принятых в установленном порядке.
Доверенный номер	Номер мобильного (сотового) телефона, предоставленный Клиентом Банку, способами, определяемыми Банком самостоятельно, фиксируемый в системах Банка и используемый Клиентом для получения электронных банковских услуг с использованием динамической аутентификации клиента.
Договор	Договор присоединения на обслуживание в системе «Onlinebank HALYK».
Закрытый ключ ЭЦП	Последовательность электронных цифровых символов, созданная на ключевом носителе либо в Облачном хранилище, зарегистрированная в Удостоверяющем центре и известная только владельцу регистрационного свидетельства, предназначенная 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 заявление на отзыв ключа ЭЦП и регистрационного свидетельства к нему.
Карт-ридер	Электронно-механическое устройство, обеспечивающее взаимодействие используемого уполномоченным лицом Клиента (Владельцем сертификата) оборудования с чипом (смарт-карта) 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, иностранное дипломатическое и консульское представительство, заключившее настоящий Договор присоединения.
Ключевой носитель	Защищенное электронное устройство, предназначенное для генерации, хранения закрытого и открытого ключей ЭЦП и выполнения криптографических операций с использованием средств криптографической защиты информации.
Колбэк (callback)	Звонок из Банка Клиенту о необходимости подтверждения транзакции. Для подтверждения транзакции Клиент называет «кодовое слово» и детали транзакции. Для подтверждения транзакции звонок Клиенту может быть осуществлен круглосуточно, включая выходные и праздничные дни.
Мобильное приложение (МП)	Приложение, установленное на Мобильном устройстве Клиента для работы в Системе. При работе через данное приложение применяются ограничения и лимиты по суммам на совершение операций в Системе. Информация по лимитам размещена на сайте www.halykbank.kz
Мобильное устройство	Планшетный компьютер, смартфон или фаблет с установленными операционными системами iOS или Android, на которое устанавливается Мобильное приложение.
НУЦ	Национальный удостоверяющий центр Республики Казахстан, предоставляющий средства надежной Аутентификации и/или электронной цифровой подписи для физических и юридических лиц Республики Казахстан при использовании сервисов электронного правительства,

	информационных систем различных бизнес-структур, а также для защиты сообщений электронной почты, и обеспечивающий выдачу регистрационных свидетельств (сертификат).
Облачная ЭЦП	Электронная цифровая подпись физического лица (уполномоченного представителя Клиента), формирующаяся в Облачном хранилище данных Системы «Certex Cloud» после регистрации через Удостоверяющий центр Банка и подтверждающая достоверность подписанного ею электронного документа, его принадлежность и неизменность содержания.
Операционный день	Часы, установленные Банком для приема платежных документов, осуществления кассовых 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 Onlinebank, который предоставляет Клиенту индивидуальный курс для сделок по конвертациям, покупке/продаже валюты на условиях, определяемых Банком.
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, смарт-карта или Java Token и/или осуществляется вход и авторизация Клиента в Системе Onlinebank.
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».
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.
Служба поддержки Интернет-банкинга	Подразделение Банка, осуществляющее обслуживание телефонных вызовов, электронных и письменных обращений и сопровождение существующих и потенциальных Клиентов Системы Onlinebank по телефону.
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.
Средства криптографической защиты информации (СКЗИ)	Совокупность программно-технических средств, реализующих алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами и обеспечивающих применение электронной цифровой подписи и шифрования в информационных системах. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.
Счет	Банковский счет Клиента в Банке в любой валюте, открытый на основании договора банковского счета, договора присоединения на открытие текущего счета в карточной базе и обслуживание корпоративной платежной карточки, 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	Подразделение Банка, осуществляющее выпуск и обслуживание ЭЦП, удостоверяющее соответствие открытого ключа ЭЦП закрытому ключу ЭЦП, а также подтверждающее достоверность и активность регистрационного свидетельства.
Уполномоченное лицо/ Уполномоченный представитель	Физическое лицо – уполномоченный представитель Клиента, на имя которого Удостоверяющим центром выдано Регистрационное свидетельство, правомерно владеющее Закрытым ключом электронной цифровой подписи, соответствующим Открытому ключу электронной цифровой подписи, указанному в Регистрационном свидетельстве.
Уполномоченный орган	Национальный Банк Республики Казахстан или иной уполномоченный государственный орган.
Устройства для аутентификации	При использовании данного термина, подразумеваются все выданные Клиенту устройства для подключения к Системе Onlinebank, указанные Клиентом в Заявлении на подключение пользователя к Системе.
Устройство eToken PASS	Автономное устройство, позволяющее Клиенту самостоятельно по запросу генерировать уникальную последовательность электронных цифровых символов (далее – Код), предназначенную для одноразового использования при авторизации электронных платежей. Для каждой авторизации в Системе Onlinebank требуется создание и использование нового одноразового (единовременного) кода.
Файловый сертификат	Регистрационное свидетельство в виде электронного документа, выдаваемое уполномоченному лицу Клиента без записи его на Ключевой носитель после подписания Соглашения на выдачу файлового сертификата по форме Приложения 7 к Договору и используемое для передачи электронных документов Клиента при интеграции учетной/бухгалтерской системы Клиента с Системой Onlinebank.
Финансовый номер	Номер мобильного (сотового) телефона, предоставленный Клиентом Банку способами, определяемыми Банком самостоятельно, фиксируемый в системах Банка и используемый для переводов денег на банковский счет Клиента.
Электронная цифровая подпись (далее – ЭЦП)	Набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания. 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 и/или подтверждена Способом динамической аутентификации.

Статья 3. Подключение Системы Onlinebank

3.1. Клиент для подключения версий Системы Onlinebank должен заполнить Заявление по форме Приложения 1 к настоящему Договору или Заявление-Анкету по форме, утвержденной в Банке (далее – «Заявление-Анкета»), и предоставить все надлежащим образом оформленные документы в соответствии с требованиями Банка.

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

3.3. Для подключения версии «Onlinebank Limit» Клиент присоединяется к настоящему Договору, соглашаясь с его условиями при регистрации в Системе и подтверждении электронной формы Заявления. Подключение к версии системы «Onlinebank Limit» возможно для Клиентов – физических лиц (индивидуальных предпринимателей), имеющих в Банке Счет и действительный сертификат НУЦ и/или доступ к порталу электронного правительства (eGov), посредством Аутентификации. Регистрация в Системе Onlinebank будет невозможна без присоединения к условиям настоящего Договора.

3.4. Подписывая заявления по формам согласно Приложениям 1, 2 к настоящему Договору или Заявление-Анкету, Клиент подтверждает, что Банк донес информацию о необходимых устройствах

Ключевого носителя и/или Способе динамической аутентификации при подключении версий Системы Onlinebank.

3.5. Клиент не может быть подключен одномоментно к двум имеющимся версиям Системы Onlinebank.

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

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

3.8. Подключение к любой версии Системы Onlinebank невозможно без указания Клиентом Доверенного номера.

3.9. 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 и другим услугам, предусмотренным в Договоре.

При изменении номера мобильного (сотового) телефона Уполномоченного лица Клиента, зарегистрированного в Системе Onlinebank в качестве Доверенного номера, или смене Уполномоченного лица Клиент предоставляет в Банк Заявление на изменение средства аутентификации согласно приложению 5 к настоящему Договору. В случае утери/кражи мобильного (сотового) телефона Уполномоченного лица Клиента, при наличии у него активированного Облачного ЭЦП, Клиент обязан в кратчайшие сроки заблокировать Уполномоченное лицо путем обращения в Службу поддержки Интернет-банкинга или обслуживающее подразделение Банка. После временного блокирования Уполномоченного лица сертификат можно отозвать либо, по желанию Клиента, разблокировать Уполномоченное лицо. Отозванный сертификат подлежит замене.

3.10. Клиент подтверждает, что при подписании Заявления Банк уведомил Клиента о существовании в Банке различных уровней безопасности при подключении Системы Onlinebank.

3.11. При выборе высокого уровня безопасности Клиент выбирает предложенное ему устройство Ключевого носителя (смарт-карту или устройство Java Token), а также один из Способов динамической аутентификации (Onlinebank-аутентификация или аутентификация с помощью Устройства eToken PASS), предлагаемых в Приложениях 1, 2 к настоящему Договору.

Клиент обязуется при первом входе в Систему Onlinebank 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 Приложениях 1, 2 к настоящему Договору Способ динамической аутентификации, будет считаться, что Клиент подключил Систему со средним уровнем безопасности, принимая все риски и не имеет никаких претензий к Банку в случае несанкционированного доступа к Системе.

3.12. При выборе Клиентом предложенного ему устройства Ключевого носителя (смарт-карту или устройство Java Token) подключается Система со средним уровнем безопасности.

3.13. При выборе Клиентом только Способа динамической аутентификации (Onlinebank-аутентификация или SMS аутентификация), без Ключевого носителя, подключается Система с низким уровнем безопасности.

3.14. Клиент подтверждает, что Банк, любыми выбранными им способами, донес информацию до Клиента о возникших рисках при подключении Системы Onlinebank и выборе среднего или низкого уровня безопасности.

3.15. Клиент при выборе среднего и низкого уровня безопасности 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.

3.16. Банк передает Клиенту выбранные Клиентом устройства при подключении в Системе Onlinebank, согласно Приложениям 1 и 2 к настоящему Договору, которые Клиент вправе использовать исключительно для получения электронных банковских услуг и иных услуг, предусмотренных в Договоре.

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

3.17. 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 Onlinebank, поломке Устройств для аутентификации и/или истечении срока действия регистрационного свидетельства Клиента, все Устройства для аутентификации

остаются у Клиента или, при желании, могут быть переданы в Банк. Банк при приеме от Клиента Устройств для аутентификации проводит обязательную очистку Ключевых носителей.

При утере Клиентом Устройств для аутентификации, Банк по инициативе Клиента повторно выдает Клиенту устройства на платной основе согласно Тарифам Банка. Ключевые носители при этом будут очищены.

3.18. Стороны соглашаются, что Устройства для аутентификации будут считаться переданными Банком Клиенту с момента подписания Сторонами акта приема-передачи (Приложение 6 к настоящему Договору).

3.19. В случае открытия Клиентом новых счетов в Банке они автоматически загружаются в Систему Onlinebank. Права Уполномоченных лиц будут автоматически действовать на вновь открытые счета. Для внесения изменений по настройке прав Уполномоченных лиц на вновь открытые счета Клиенту необходимо будет обратиться в Банк.

3.20. Физические лица, которые будут вправе подписывать Электронные документы Клиента в качестве уполномоченных лиц Клиента, будут определяться исходя из представленных Клиентом в Банк заявлений по форме согласно Приложениям 1 и 2 к настоящему Договору или Заявления-Анкеты, где для подключения к Системе Onlinebank указан доверенный номер первого руководителя, либо по заявлению на привязку пользователя согласно Приложению 3 к настоящему Договору. Заявление на привязку пользователя (Приложение 3 к настоящему Договору) заполняется Клиентом в случае, если Уполномоченное лицо, которому Клиент предоставляет право подписания своих электронных документов, уже имеет ЭЦП Удостоверяющего центра и выпуск нового сертификата не требуется. Каждое представленное Клиентом заявление будет являться неотъемлемой частью Договора.

3.21. Клиент выражает согласие, что Уполномоченное лицо, которому в соответствии с заявлением предоставлено право подписи с использованием ЭЦП и/или одним из способов динамической аутентификации, может совершать операции, действия, подписывать документы, в том числе для совершения сделок, с использованием регистрационного свидетельства физического лица – Облачной ЭЦП. Электронные документы, используемые при совершении операций в Системе Onlinebank и/или посредством Мобильного приложения, подписанные Облачной ЭЦП, равнозначны документам на бумажном носителе и порождают аналогичные им права и обязанности Сторон.

3.22. Клиент заверяет Банк, что указанное в Приложениях 1, 2 или 3 к настоящему Договору Уполномоченное лицо будет совершать операции, действия, подписывать документы, включая документы для совершения сделок, не только в соответствии с доверенностью, выданной ему Клиентом, но и при наличии у Клиента:

- предварительного решения соответствующего органа/должностного лица Клиента, если такое решение необходимо для совершения Клиентом операций, действий, подписания документов в соответствии с его внутренними процедурами, требованиями третьих лиц, требованиями законодательства, какими-либо иными требованиями, которые Клиент обязан исполнять, соблюдать, и/или

- решения, разрешения, согласия, одобрения, уведомления соответствующего государственного органа и/или уполномоченного государством лица, наличие которого может являться необходимым условием совершения Клиентом операций, действий, подписания документов между Клиентом и Банком, включая совершение сделки между ними, а также исполнения Клиентом своих обязательств по ним.

3.23. Клиент заверяет, что при расширении Банком перечня операций, которые могут осуществляться посредством Системы Onlinebank с использованием электронных документов, Клиент выдаст доверенность указанному Уполномоченному лицу с полномочиями на совершение новых операций с использованием электронной цифровой подписи. Перечисленные выше заверения Клиента распространяются также и на новые операции. Клиент заверяет, что у него существует надлежащая система контроля за использованием лицами, наделенными им правом подписи с использованием ЭЦП и/или одного из Способов динамической аутентификации, полномочий по использованию ЭЦП и/или одного из Способов динамической аутентификации.

Статья 4. Оказание услуг в Системе Onlinebank

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

4.2. 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.

4.3. Информация на Ключевом носителе и/или сгенерированный, одноразовый (единовременный) код, Pin-код являются конфиденциальными. В случае, разглашения Клиентом данной информации третьим лицам, Банк не несет ответственность за понесенные ущербы, убытки Клиента.

4.4. Клиент имеет возможность использования Системы Onlinebank вне зависимости от времени и/или даты. Электронные документы могут быть отправлены Клиентом в Банк для исполнения также в любое время. При этом обработка и исполнение Банком принятых Электронных документов в адрес контрагентов, не являющихся клиентами Банка, возможны только в течение Операционного дня.

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.

4.5. Банк приостанавливает предоставление электронных банковских услуг и иных услуг, предусмотренных в Договоре, по причине неисправности технических средств, обеспечивающих предоставление электронных банковских услуг и иных услуг. При устранении причин, повлекших приостановление предоставления электронных банковских услуг и иных услуг, Банк возобновляет предоставление Клиенту электронных банковских услуг и иных услуг по Договору.

4.6. Для работы в Системе Onlinebank 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 10 и выше, Mac OS последней версии;
- браузер Microsoft Internet Explorer не ниже 11 версии, Chrome, Mozilla, Opera последних версий;
- 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;
- TUMAR-CSP.

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.

4.7. Перечень операций, которые могут осуществляться посредством Системы Onlinebank 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;

2) прием и отправка переводов на Финансовый номер;

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

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

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

6) предоставление Клиенту в электронном виде выписок по счетам:

– финальной выписки о состоянии Счета;

– предварительной выписки;

– по сберегательным счетам;

– по сберегательным счетам (условия депозита, дата открытия/закрытия, срок действия);

– по корпоративному карт-счету в разрезе корпоративных карт;

7) предоставление Клиенту справок в электронном виде (о наличии счета, об остатках по счету, об оборотах по счетам за период);

8) 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;

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

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

11) запросы на выпуск регистрационных свидетельств;

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

13) пополнение счета в Автокассе, снятие денег через банкомат и Автокассу;

14) настройка автосальдирования счета;

15) установка 3D Secure/Secure Code – секретного пароля, используемого в процессе проведения карточной операции в режиме on-line через Интернет;

16) прием заявления на установку кредитного лимита;

17) прием заявления на снятие лимитов по корпоративным карточкам;

18) прием заявления на новый QR-код;

19) бронирование электронной очереди в отделении Банка;

20) уведомления о поступлении/зачислении валюты;

21) 1С Direct Bank – интеграция с «1С-Бухгалтерия» Клиента;

22) веб-сервис – интеграция с бухгалтерской/учетной системой Клиента посредством технологии API. Доступ к веб-сервису Банка предоставляется с использованием файлового сертификата Клиента, который выпускается на уполномоченное лицо Клиента согласно сопроводительного письма. Интеграция с бухгалтерской/ учетной системой Клиента осуществляется ресурсами Клиента;

23) выпуск корпоративных платежных карточек;

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

Перечень доступных операций зависит от версии Системы, выбранной Клиентом.

В «Onlinebank Start» доступны налоговые, социальные и пенсионные платежи, просмотр/выгрузка выписок по своим счетам, конвертация валюты и переводы между своими счетами, перечисление заработной платы и других выплат на текущие/карт-счета без ограничений, выпуск корпоративных платежных карточек, а также проведение платежей в пользу контрагентов, в том числе прием и отправка переводов на Финансовый номер, в пределах лимита по общей сумме и по количеству платежей в месяц. Лимит на проведение платежей в тенге может быть увеличен Клиентом при оплате Клиентом данной услуги по Тарифам Банка, указанным на сайте www.halykbank.kz. Также Клиенту доступно проведение электронных документов в валюте, предоставление в электронном виде валютного контроля, информация по возвратам платежей и кассовые операции по приему и снятию наличных денег со счета через Автокассу и банкомат.

В «Onlinebank Limit» доступно проведение пенсионных, социальных, страховых и налоговых выплат, просмотр/выгрузка выписок по своим счетам, бронирование очереди, конвертация валюты, зачисление валютного перевода, информация по возвратам платежей и переводы между своими счетами без санкционирования Банком в пределах установленного лимита, а также проведение платежей в пользу контрагентов только через санкционирование специалистом по обслуживанию юридических лиц ЦБ/ЦБО/РУ при проверке оригинала платежного документа с подписью и печатью Клиента при ее наличии. По всем платежам в тенге имеются ограничения как по количеству, так и по сумме (лимит). 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.

4.8. 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 курс 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 условиями;

3) при заведении одним Клиентом нескольких заявок на конвертацию, но не подписанными и не отправленными в Банк по истечении текущего операционного дня, на систематических условиях, Банк вправе отключить платформу «Halyk FX» у данного Клиента;

4) Банк вправе устанавливать лимиты на проведение конвертаций, инициированных Клиентом во внеоперационное время.

4.9. Банком предусмотрена возможность интеграции учетной/ бухгалтерской системы Клиента для передачи и получения электронных документов посредством использования Клиентом регистрационного свидетельства в виде электронного документа - файлового сертификата, при этом Клиенту передается документ без записи его на Ключевой носитель. Выдача файлового сертификата осуществляется после подписания Клиентом Соглашения по форме Приложения 7 к настоящему Договору. Так как файловый сертификат защищен только паролем, все риски, связанные с возможным несанкционированным использованием файловых сертификатов, регистрируемых и используемых для подписания электронных документов Клиента, несет Клиент.

Передача Банком Клиенту файлового сертификата осуществляется в течение 10 (десяти) рабочих дней с момента его выпуска Удостоверяющим центром, и оформляется Актом приема-передачи файлового сертификата, форма которого приведена в приложении 1 к Соглашению.

4.10. 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.

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.

4.11. 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.

4.12. Стороны взаимно обязуются принимать на себя в полном объеме все обязательства, вытекающие из электронных документов, подписанных одним из Способов динамической аутентификации и/ или подписанных 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.

4.13. Клиент признает, что закрытые ключи ЭЦП находятся на ключевом носителе (Облачной ЭЦП – в базе Certex Cloud) и выпущены в единственном экземпляре.

4.14. 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 Onlinebank. Банк имеет право не хранить документы сроком более одного года с учетом требований Действующего законодательства.

Банк не осуществляет распечатку электронных документов на бумажном носителе с целью их хранения или передачи Клиенту. Распечатка электронных документов на бумажном носителе осуществляется по запросу Клиента, за каждый экземпляр Банк взимает комиссионное вознаграждение в соответствии с действующими Тарифами.

4.15. 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 версии «Onlinebank Business» или автоматически при подключении версий Системы «Onlinebank Start».

4.16. 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;
- доступ в интернет.

Использование Облачной ЭЦП в Мобильном приложении возможно только после процедуры Верификации мобильного устройства. Без Верификации мобильного устройства функционал Мобильного приложения может быть использован с установленным Банком суточным ограничением (лимитом) Клиента по сумме Электронных документов, отправленных на исполнение в Банк. Информация о лимите размещена на сайте www.halykbank.kz.

При Верификации мобильного устройства присваивается токен для мобильного устройства. Далее авторизация в Мобильном приложении осуществляется путем ввода Клиентом Pin-кода или при помощи средств биометрической аутентификации (отпечаток пальца, изображение лица).

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

4.18. В случае, если Клиент не обратился в Банк для получения Ключевых носителей и/или за устройством, необходимым для Способа динамической аутентификации, в течение 45 календарных дней после выпуска Регистрационного свидетельства для подключения к Системе Onlinebank, Банк не выдает Ключевые носители и/или устройство, необходимое для выбранного Способа динамической аутентификации, при этом, комиссия за подключение к Системе Onlinebank взимается в соответствии с Тарифами Банка.

Статья 5. Обеспечение безопасности

5.1. Клиент соглашается следовать процедурам безопасности и любым другим инструкциям, предоставляемым Банком Клиенту относительно безопасности Системы Onlinebank.

5.2. 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 Систему Onlinebank.

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

Клиент обязуется не разглашать Pin-код третьим лицам, а также обеспечить невозможность доступа к нему.

5.4. 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.

5.5. Клиент обязуется бережно относиться к устройствам, переданным ему Банком:

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

А также обязуется 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.

5.6. 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. Подробнее о мерах безопасности Клиент может ознакомиться на странице Системы Onlinebank https://halyk.onlinebank.kz/wiki/.

Статья 6. Услуга SMS-информирования

6.1. Для получения информации о платежах посредством SMS-информирования на Доверенный номер, Клиент самостоятельно направляет запрос на подключение посредством Системы Onlinebank.

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

6.3. 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 услуге 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 Клиентом при подписании заявления по форме Приложений 1, 2 или 3 к настоящему Договору или Заявления-Анкеты.

Статья 7. Комиссионное вознаграждение Банка

7.1. 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.

7.2. Тарифы размещаются на сайте Банка по адресу www.halykbank.kz. Об изменениях, дополнениях в тарифы Банк уведомляет Клиента посредством размещения информации на сайте Банка по адресу www.halykbank.kz не менее чем за 10 (десять) рабочих дней до даты введения в действие таких изменений, дополнений, с указанием в уведомлении права Клиента до даты, с которой будут введены в действие такие изменения, дополнения, отказаться от Договора (расторгнуть Договор) без уплаты дополнительной комиссии за его расторжение.

7.3. 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 8. Обязанности и права Сторон. Персональные данные.

8.1. 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 Системе Onlinebank и Сторонам;

– не разглашать третьей стороне (за исключением случаев, предусмотренных действующим законодательством или дополнительным соглашением Сторон) конкретные способы защиты информации, применяемые в Системе Onlinebank, 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 Системы Onlinebank, 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 либо заблокировать пользователя, на которого выпущен ключ, путем обращения в Службу поддержки Интернет-банкинга или обслуживающее подразделение Банка;

– в случае получения письменного уведомления со стороны Клиента о подозрении на несанкционированный доступ в Систему Onlinebank, 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.

8.2. Банк имеет право:

– отказать в приеме электронных документов к исполнению по основаниям, предусмотренным в Договоре;

– вносить изменения в механизмы защиты Системы Onlinebank 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 Системе Onlinebank;

– блокировать доступ Клиента в Систему Onlinebank в случае истечения срока действия регистрационного свидетельства Клиента;

– блокировать доступ Клиента в Систему Onlinebank 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 Счету и отсутствия денег на Счете более шести месяцев подряд расторгнуть Договор путем отказа от Договора;

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

– блокировать доступ Клиента в Систему Onlinebank 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 Onlinebank - аутентификацией;

– блокировать доступ Уполномоченного представителя Клиента в Систему Onlinebank в случае обращения учредителей/руководителя Клиента по вопросу отказа в предоставлении доступа уполномоченному лицу Клиента с условием представления документов, подтверждающих смену Уполномоченного представителя (решения, приказа о назначении, заявления на отключение пользователя от Системы Onlinebank), в течение Операционного дня с момента блокирования доступа. После предоставления подтверждающих документов Банк осуществляет процедуры по отзыву сертификата. В случае непредставления в течение указанного срока подтверждающих документов Банк вправе разблокировать доступ Уполномоченному представителю Клиента;

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

– отказать в установлении деловых отношений с Клиентом в случае невозможности принятия мер по надлежащей проверке, предусмотренных Действующим законодательством и внутренними документами Банка, а также в случае наличия подозрений о том, что деловые отношения используются Клиентом в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

– требовать от Клиента (его представителя) представления сведений и документов, необходимых для идентификации Клиента (его представителя), выявления бенефициарного собственника, а также предоставления сведений о налоговом резидентстве, роде деятельности и источнике финансирования совершаемых операций;

– отказать в приеме электронных документов к исполнению по основаниям, предусмотренным в Договоре;

– не принимать к обработке электронные документы по основаниям, но не ограничивая себя, предусмотренным в условиях Договора;

– приостановить исполнение расходных операций по счету в случае возникновения подозрений о том, что такие операции совершаются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

– прекратить деловые отношения с Клиентом путем одностороннего отказа от исполнения Договора в случаях:

возникновения в процессе изучения операций подозрений о том, что деловые отношения используются Клиентом в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

неоднократных отказов в проведении расходных операций по Счету либо приостановления всех операций по банковским счетам Клиента;

наличия санкций в отношении Клиента и (или) их аффилированных лиц, наложенных в соответствии с юрисдикцией любой страны (например, OFAC) или международной организации (включая, но не ограничиваясь, FATF и ООН);

наличия у Банка оснований полагать, что операции Клиента/контрагента Клиента попадают под действие международных экономических санкций либо направлены на уклонение от международных экономических санкций;

предусмотренных внутренними документами и процедурами Банка о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

– пользоваться другими правами, предусмотренными Договором, Действующим законодательством.

8.3. Банк обязан:

– после заключения настоящего Договора и оплаты Клиентом надлежащих комиссий, в соответствии с Тарифами Банка, зарегистрировать Клиента в Системе Onlinebank, передать Клиенту Ключевой носитель, Карт-ридер, в случае выбора Ключевого носителя – смарт-карты и устройство eToken PASS, в случае выбора Клиентом данного Способа динамической аутентификации, для начала работы с Системой Onlinebank;

– предоставлять электронные банковские услуги и другие услуги, предусмотренные в Договоре, 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 Системы Onlinebank в соответствии с Тарифами Банка;

– исполнять другие обязанности, предусмотренные Договором, Действующим законодательством.

8.4. Клиент обязан:

– изучить условия настоящего Договора и следовать описанным в ней рекомендациям Банка;

– 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;

– 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 настоящим Договором;

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

– по окончании рабочей сессии в Системе Onlinebank – 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 Системе, и незамедлительно отозвать их регистрационные свидетельства 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-информировании;

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

– немедленно обратиться в Банк с заявлением на отзыв регистрационного свидетельства либо блокирование пользователя 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, Рабочем месте и/или не разглашать сгенерированный единовременный (одноразовый) код;

– после первого входа в Систему Onlinebank 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 Onlinebank электронный запрос в Удостоверяющий центр на автоматическое продление срока;

– в случае изменения информации, указанной в документах, предоставленных Клиентом при подаче заявления на подключение, представить документы, подтверждающие такие изменения;

– предоставлять в Банк информацию и документы, необходимые для исполнения Банком обязанностей, предусмотренных Действующим законодательством и внутренними документами Банка, включая информацию о бенефициарных собственниках;

– осуществлять операции и получать наличные деньги/пополнять счет через Автокассу и (или) Cash by code только непосредственно самим Клиентом либо уполномоченными лицами Клиента, то есть лицами, имеющими в установленном Действующим законодательством порядке ЭЦП, а также прошедших процедуру идентификации в Банке и которые сами санкционировали операцию в Системе Onlinebank посредством подписания заявки своими ЭЦП;

- не передавать третьим лицам право пользования сгенерированным кодом/штрихкодом по продукту Cash by code, Автокасса;

- немедленно уведомлять Банк о наделении Уполномоченного лица/Уполномоченных лиц полномочиями на распоряжение Счетом;

- указывать торговое наименование бизнеса и логотип при регистрации Финансового номера и не использовать слова/словосочетания, которые бы могли нанести вред деловой репутации Банка и/или третьих лиц, в соответствии с законодательством Республики Казахстан;

- исполнять другие обязанности, предусмотренные Договором, Действующим законодательством.

8.5. Клиент имеет право:

– обслуживаться в Системе Onlinebank в соответствии с условиями настоящего Договора;

– выбрать версию Системы Onlinebank, 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 в соответствии с действующими Тарифами;

– требовать от Банка надлежащего исполнения условий настоящего Договора;

– пользоваться другими правами, предусмотренными Договором, Действующим законодательством.

8.6. 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 и/или Заявление-Анкету, 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 том числе 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) Организациям 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.

8.7. Настоящим Клиент заверяет, что в отношении персональных данных субъектов персональных данных, переданных и подлежащих передаче в будущем Клиентом Банку и (или) Организациям 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 том числе Банку и (или) Организациям, обработку Банком и (или) Организациями персональных данных.

8.8. 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 том числе 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.

8.9. Ответственность за отсутствие согласий на сбор и обработку персональных данных, на передачу персональных данных третьему лицу, в том числе 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.

8.10. Настоящим Клиент предоставляет Банку согласие на раскрытие Банком сведений, составляющих банковскую тайну Клиента, отправителю денег в случаях зачисления на банковский счет Клиента денег, поступивших от отправителя с использованием перевода по Финансовому номеру Клиента. Раскрытие Банком указанных выше сведений выражается в указании номера счета Клиента (ИИК) в выписке, получаемой отправителем денег после зачисления суммы перевода, отправленного им на банковский счет Клиента.

Статья 9. Ответственность Сторон

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

9.2. 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.

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

9.4. За сохранность и защиту от несанкционированного доступа третьих лиц к сертификатам Облачной ЭЦП, хранящимся на сервере Банка в Облачном хранилище данных Системы «Certex Cloud», Банк несет полную ответственность в соответствии с условиями Договора.

9.5. 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, Мобильное устройство с активированной Облачной ЭЦП,

Ключевой носитель, в случае подключения Системы Onlinebank 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.

9.6. 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 подключении пользователей, лиц, уполномоченных инициировать, подтверждать, направлять сообщения (указания) посредством Системы Onlinebank.

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

9.8. Ответственность за отсутствие согласий на сбор и обработку персональных данных на передачу персональных данных третьему лицу, в том числе Банку, Организациям, возлагается на Клиента. Клиент несет ответственность за отсутствие согласий субъектов персональных данных на осуществление Банком трансграничной передачи их персональных данных. В случае применения к Банку каких-либо мер за нарушение действующего законодательства Республики Казахстан о персональных данных и их защите Клиент обязуется возместить Банку, по требованию Банка, любые, понесенные Банком расходы и убытки.

9.9. Клиент несет полную ответственность за понесенные убытки в случае несанкционированного доступа к Мобильному устройству владельца сертификата, которое используется для входа в Мобильное приложение и отправки Электронных документов.

9.10. Клиент несет полную ответственность в случае несанкционированного доступа третьих лиц к сгенерированному коду/штрих-коду для проведения операций по продукту Cash by code/Автокасса, а также за изъятие третьими лицами наличных денег/пополнение Счета посредством сгенерированного кода/штрих-кода. В случае несоблюдения данного условия, Банк не несет ответственность за понесенные Клиентом убытки и не возмещает их Клиенту.

9.11. Отдельные вопросы об убытках, ущербе могут регулироваться в других статьях Договора.

Статья 10. Разрешение споров

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

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

10.3. 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.

10.4. 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 Onlinebank (если сообщение (указание) было инициировано без использования Ключевого носителя) и при необходимости – представитель разработчика Системы Onlinebank, 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 Onlinebank.

10.5. 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 Onlinebank, 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 динамической 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 динамической аутентификации;
- извлечение данных и ЭЦП электронного документа из архива базы данных Системы Onlinebank и проверка подлинности ЭЦП Клиента/извлечение сообщения (указания) из архива базы данных Системы Onlinebank и проверка надлежащего порядка инициирования, подтверждения сообщения (указания).

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

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

10.7. 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.

Статья 11. Форс-мажор

11.1. 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.

11.2. 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.

11.3. 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 12. Действие Договора. Язык Договора

12.1. Договор вступает в силу с момента присоединения Клиента к условиям Договора путем подписания Заявления на подключение к Системе (Приложение 1 к настоящему Договору) и/или Заявления-Анкеты.

12.2. Договор действует бессрочно.

12.3. Договор расторгается:

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

12.3.2. 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 Системы Onlinebank, 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;

12.3.3. 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 Договоре, не ограничивая при этом право каждой из Сторон отказаться от Договора в других случаях.

Статья 13. Заключительные положения

13.1. 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.

13.2. 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 и других услуг, предусмотренных в Договоре, с использованием Системы Onlinebank.

13.3. 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 Системы Onlinebank, 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 срока, указанного в части первой настоящего пункта, 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 электронной почтой – в день отправки;

4) при отправке посредством Системы Onlinebank – 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 электронной почтой – в день отправки;

4) при отправке посредством Системы Onlinebank – в день отправки.

13.4. 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.

13.5. 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.

Приложение 1
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ КЛИЕНТА/ПОЛЬЗОВАТЕЛЯ К СИСТЕМЕ И ПРИСОЕДИНЕНИЕ К ДОГОВОРУ И РЕГЛАМЕНТУ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «НАРОДНЫЙ БАНК КАЗАХСТАНА»

Наименование Клиента: _____

БИН/ИИН: _____

Контактный мобильный номер Клиента[1]: +7 ☐☐☐☐☐☐☐☐☐☐

Выбор версии системы Onlinebank: ☐ **Business** ☐ **Start**

☐ Для удалённого доступа ко всем счетам Клиента[2]

Примечания[3]:

☐ Отключить от текущей версии ☐ Сделать перенос архива

Настоящим Клиент подтверждает:
что ознакомился со всеми условиями Договора присоединения на обслуживание в системе «Onlinebank HALYK» (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 Договору в целом и дает согласие Банку на их изменение и дополнение в порядке, установленном в Договоре;
что ознакомился со всеми условиями Регламента Удостоверяющего центра АО «Народный Банк Казахстана» (далее - Регламент), размещенного по ссылке Регламент Удостоверяющего центра Народного Банка 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 Регламенту в целом и дает согласие Банку на их изменение и дополнение в порядке, установленном в Регламенте;
наличие программно-технических средств, указанных в п. 4.6 Договора, и просит предоставить доступ к системе «Onlinebank HALYK».

Просим предоставить доступ к Системе Onlinebank и изготовить криптографические ключи и регистрационное свидетельство открытого криптографического ключа для пользователя:

Уполномоченное лицо (*указывается на латинице для нерезидентов*)	Фамилия_____ Имя_____ Отчество (при наличии) _____
Документ, удостоверяющий личность	вид документа: _____ номер: _____ серия: _____ орган, выдавший документ: _____ дата выдачи: «____» _____20___г. срок действия: «____» _____20__г. ИИН: (при наличии)_____
Контактные данные	Доверенный номер[4]: +7 ☐☐☐☐☐☐☐☐☐☐ Email: _____
Выбор способа аутентификации и Ключевого носителя для версии Business	*Выберите Ключевой носитель:* ☐ Java Token ☐ Смарт-карта *Выберите Способ динамической аутентификации:* ☐ Устройство eToken PASS ☐ Online-аутентификатор
Право подписи	☐ без права подписи ☐ право _____ подписи[5]
Реквизиты доверенности	

[1] Указывается мобильный номер Клиента, на который придет SMS о подключении и готовности Ключевых носителей.
[2] В случае предоставления удаленного доступа на индивидуальных условиях необходимо дополнительное письмо Клиента.
[3] Данные отметки проставляются при переходе Клиента на другую версию Системы.
[4] Поле «Доверенный номер» обязательно для заполнения, оно используется для SMS-аутентификации, SMS-информирования и получения OTP-пароля.
[5] Возможно указание от 1 до 3 уровней подписания документов.

Настоящим Клиент заверяет Банк, что лицо, которому в соответствии с заявлением Клиент предоставляет право подписи с использованием ЭЦП, имеет в выданной ему Клиентом доверенности необходимые полномочия для совершения операций, действий, подписания документов, включая документы для совершения между Клиентом и Банком сделок, с использованием электронной цифровой подписи. Настоящим Клиент гарантирует Банку, что по первому требованию Банка и в срок, указанный Банком, в зависимости от необходимости, определяемой самостоятельно Банком, предоставит Банку, в том числе через указанное выше лицо, любые из указанных выше документов (доверенность, решение, разрешение, согласие, одобрение, уведомление). Настоящим Клиент безусловно соглашается, что в случае невозможности представления им самим и/или указанным выше лицом затребованных Банком документов, включая доверенность, и/или в случае совершения указанным выше лицом с Банком сделки без доверенности, без соответствующих полномочий в доверенности, совершение Клиентом, включая указанное выше лицо, действий по осуществлению любого из прав, исполнению любой из обязанностей, предусмотренных сделкой, принятие Клиентом от Банка и/или Банком от Клиента какого-либо исполнения по сделке, исполнение в рамках сделки Клиентом и/или Банком любого из требований Банка, Клиента, соответственно, будет считаться, что совершенная указанным выше лицом с Банком сделка считается одобренной Клиентом согласно статье 165 Гражданского кодекса Республики Казахстан и действительной для Клиента с момента ее совершения без необходимости представления Клиентом отдельного документа об одобрении сделки. Клиент выражает согласие, что уполномоченное лицо, которому в соответствии с данным заявлением предоставлено право подписи с использованием ЭЦП и/или одним из способов динамической аутентификации, может совершать операции, действия, подписывать документы, в том числе для совершения сделок, с использованием регистрационного свидетельства физического лица – облачной ЭЦП.	
Области использования регистрационного свидетельства (объектные идентификаторы, определяющие отношения, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение): 1. Цифровая подпись 2. Неотрекаемость	
Срок действия регистрационного свидетельства	**1 (один) год**

Необходим картридер в количестве _____ шт.

Первая подпись *Первый руководитель*	Должность _____ Ф.И.О. _____	Подпись	Печать при наличии
Вторая подпись *Главный бухгалтер*	Должность _____ Ф.И.О. _____	Подпись	
Дата заполнения заявления	«_____» _____ 20_____ г. *День* *Месяц* *Год*		

Данные о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи, и обозначение стандарта алгоритма электронной цифровой подписи: “ТУМАР-CSP”; ГОСТ 34.310-2004.

Отметки Банка

Номер устройства eToken PASS[6]	
Заявление принял *Работник Банка*	Ф.И.О. _____ Подпись _____
Наименование филиала	
Руководитель	Ф.И.О. _____ Подпись _____

[6] Заполняется работником Банка при выдаче Клиенту устройства eTokenPASS

Приложение 2
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ ПОЛЬЗОВАТЕЛЯ К СИСТЕМЕ

Наименование Клиента: _____

БИН/ИИН: _____

☐ **ВЫПУСК** ☐ **ПЕРЕВЫПУСК**[7]

Просим предоставить доступ к Системе Onlinebank и изготовить криптографические ключи и регистрационное свидетельство открытого криптографического ключа для пользователя:

Уполномоченное лицо (*указывается на латинице для нерезидентов*)	Фамилия_____ Имя_____ Отчество (при наличии) _____
Документ, удостоверяющий личность	вид документа: _____ номер: _____ серия: _____ орган, выдавший документ: _____ дата выдачи: «____» _____20___г. срок действия: «____» _____20__г. ИИН: (при наличии)_____
Контактные данные	Доверенный номер[8]: +7 ☐☐☐☐☐☐☐☐☐☐ Email: _____
Выбор способа аутентификации и Ключевого носителя для версии Business	*Выберите Ключевой носитель:* ☐ Java Token ☐ Смарт-карта *Выберите Способ динамической аутентификации:* ☐ Устройство eToken PASS ☐ Online-аутентификатор
Право подписи	☐ без права подписи ☐ право _____ подписи[9]
Реквизиты доверенности	

Настоящим Клиент заверяет Банк, что лицо, которому в соответствии с заявлением Клиент предоставляет право подписи с использованием ЭЦП, имеет в выданной ему Клиентом доверенности необходимые полномочия для совершения операций, действий, подписания документов, включая документы для совершения между Клиентом и Банком сделок, с использованием электронной цифровой подписи.

Настоящим Клиент гарантирует Банку, что по первому требованию Банка и в срок, указанный Банком, в зависимости от необходимости, определяемой самостоятельно Банком, предоставит Банку, в том числе через указанное выше лицо, любые из указанных выше документов (доверенность, решение, разрешение, согласие, одобрение, уведомление). Настоящим Клиент безусловно соглашается, что в случае невозможности представления им самим и/или указанным выше лицом затребованных Банком документов, включая доверенность, и/или в случае совершения указанным выше лицом с Банком сделки без доверенности, без соответствующих полномочий в доверенности, совершение Клиентом, включая указанное выше лицо, действий по осуществлению любого из прав, исполнению любой из обязанностей, предусмотренных сделкой, принятие Клиентом от Банка и/или Банком от Клиента какого-либо исполнения по сделке, исполнение в рамках сделки Клиентом и/или Банком любого из требований Банка, Клиента, соответственно, будет считаться, что совершенная указанным выше лицом с Банком сделка считается одобренной Клиентом согласно статье 165 Гражданского кодекса Республики Казахстан и действительной для Клиента с момента ее совершения без необходимости представления Клиентом отдельного документа об одобрении сделки.

Клиент выражает согласие, что уполномоченное лицо, которому в соответствии с данным заявлением предоставлено право подписи с использованием ЭЦП и/или одним из способов динамической аутентификации, может совершать операции, действия, подписывать документы, в том числе для совершения сделок, с использованием регистрационного свидетельства физического лица – облачной ЭЦП.

Области использования регистрационного свидетельства (объектные идентификаторы, определяющие отношения, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение):

3. Цифровая подпись
4. Неотрекаемость

Срок действия регистрационного свидетельства	1 (один) год

Необходим картридер в количестве _____ шт.

[7] При перевыпуске регистрационного свидетельства действующий ключ будет аннулирован и выпущен новый ключ.

[8] Поле «Доверенный номер» обязательно для заполнения, оно используется для SMS-аутентификации, SMS-информирования и получения OTP-пароля.

[9] Возможно указание от 1 до 3 уровней подписания документов.

Первая подпись *Первый руководитель*	Должность _____ Ф.И.О. _____	Подпись	Печать при наличии
Вторая подпись *Главный бухгалтер*	Должность _____ Ф.И.О. _____	Подпись	
Дата заполнения заявления	«_____» _____ 20_____ г. *День* *Месяц* *Год*		

Данные о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи, и обозначение стандарта алгоритма электронной цифровой подписи: “ТУМАР-CSP”; ГОСТ 34.310-2004.

Отметки Банка

Номер устройства eToken PASS[10]	
Номер контракта, к которому подключается пользователь[11]	
Заявление принял *Работник Банка*	Ф.И.О. _____ Подпись _____
Наименование филиала	
Руководитель	Ф.И.О. _____ Подпись _____

[10] Заполняется работником Банка при выдаче Клиенту устройства eTokenPASS.
[11] Указывается в случае наличия у Клиента нескольких контрактов.

Приложение 3
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

ЗАЯВЛЕНИЕ НА ПРИВЯЗКУ ПОЛЬЗОВАТЕЛЯ

Наименование Клиента: _____
БИН/ИИН: _____

Просим предоставить доступ к Системе Onlinebank пользователю:

Уполномоченное лицо (*указывается на латинице для нерезидентов*)	Фамилия_____ Имя_____ Отчество (при наличии) _____ ИИН (при наличии): _____
Наименование, БИН/ИИН организации, на которую изначально был выпущен ключ	_____ _____
Право подписи	☐ без права подписи ☐ право _____ подписи[12]
Причина предоставления права подписи	

☐Для удалённого доступа ко всем счетам Клиента[13]

☐Для удалённого доступа к нижеперечисленным счетам:

№	Номер счета	Валюта счета
1		
2		
3		

Первая подпись *Первый руководитель*	Должность _____ Ф.И.О. _____	Подпись	Печать при наличии
Вторая подпись *Главный бухгалтер*	Должность _____ Ф.И.О. _____	Подпись	
Дата заполнения заявления	«_____» _____ 20_____ г. *День* *Месяц* *Год*		

Отметки Банка

Серийный номер и дата выдачи регистрационного свидетельства	_____ «____» _____ _____г.
Заявление принял *Работник Банка*	Ф.И.О. _____ Подпись _____
Наименование филиала	
Руководитель	Ф.И.О. _____ Подпись _____

[12] Возможно указание от 1 до 3 уровней подписания документов.
[13] В случае предоставления удаленного доступа ко всем счетам Клиента номера счетов не указываются.

Приложение 4
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

ЗАЯВЛЕНИЕ НА ОТКЛЮЧЕНИЕ ПОЛЬЗОВАТЕЛЯ ОТ СИСТЕМЫ И (ИЛИ) ОТЗЫВ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА/РАСТОРЖЕНИЕ ДОГОВОРА

Наименование Клиента: _____

БИН/ИИН: _____

Причина отзыва свидетельства о регистрации/отключения от системы:
_____
(компрометация закрытого ключа, прекращение работы и т.д.)

☐ ***Просим отозвать (аннулировать) регистрационное свидетельство*** *(в случае отзыва свидетельства пользователь будет отключен от всех подключенных к нему Клиентов/компаний)*	Данные уполномоченного лица: Фамилия_____ Имя_____ Отчество (при наличии) _____ ИИН _____
☐ ***Просим отключить пользователя*** *(в случае отключения пользователь будет отключен только от указанного Клиента/компании)*	

☐	***Просим расторгнуть Договор присоединения на обслуживание в системе Onlinebank HALYK и отключить Клиента от системы:*** *(в случае расторжения договора отключаются все уполномоченные лица Клиента)*

Первая подпись *Первый руководитель*	Должность _____ Ф.И.О. _____	Подпись	Печать при наличии
Вторая подпись *Главный бухгалтер*	Должность _____ Ф.И.О. _____	Подпись	
Дата заполнения заявления	«_____» _____ 20_____ г. *День* *Месяц* *Год*		

Отметки Банка

Серийный номер и дата выдачи регистрационного свидетельства *(заполняется только в случае отзыва сертификата пользователя)*	_____ «____» _____ _____г.
Заявление принял *Работник Банка*	Ф.И.О. _____ Подпись _____
Наименование филиала	
Руководитель	Ф.И.О. _____ Подпись _____

Приложение 5
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

ЗАЯВЛЕНИЕ НА ИЗМЕНЕНИЕ СРЕДСТВА АУТЕНТИФИКАЦИИ

Полное наименование Клиента: _____

БИН/ИИН: _____

Пользователь _____
(ФИО, ИИН)

Выберите средство аутентификации, которое необходимо изменить:

☐ **Доверенный (мобильный) номер** ☐ **eToken PASS**

ИЗМЕНИТЬ

☐ **на Доверенный (мобильный) номер:**

+7										

☐ **на eToken PASS:**

Первая подпись *Первый руководитель*	Должность _____ Ф.И.О. _____	Подпись	Печать при наличии
Вторая подпись *Главный бухгалтер*	Должность _____ Ф.И.О. _____	Подпись	
Дата заполнения заявления	«_____» _____ 20_____ г. *День* *Месяц* *Год*		

Отметки Банка

Номер устройства eToken PASS[14]	
Заявление принял *Работник Банка*	Ф.И.О. _____ Подпись _____
Наименование филиала	
Руководитель	Ф.И.О. _____ Подпись _____

[14] Заполняется работником Банка при выдаче Клиенту устройства eTokenPASS

Приложение 6
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

АКТ ПРИЕМА-ПЕРЕДАЧИ

г._____ «_____»_____20____г.

Мы, нижеподписавшиеся, подтверждаем передачу Устройств, указаных в заявлении на подключение клиента к системе Onlinebank HALYK версии Business (далее – Система), согласно Приложению 2 к Договору (далее – Приложение).

Ключевой носитель _____ шт.

Картридер _____ шт.

Устройство eToken PASS _____ шт. № _____

Наименование Клиента: _____

БИН/ИИН: _____

Данные уполномоченного лица Клиента:

Фамилия_____

Имя_____

Отчество (при наличии) _____

ИИН _____

Передал:	**Принял:**
Работник Банка, передавший Устройства, выбранные Клиентом для подключения к Системе, и регистрационное свидетельство	Уполномоченное лицо Клиента, получившее Устройства, выбранные Клиентом для подключения к Системе, и регистрационное свидетельство
Должность_____ Ф.И.О. _____ Подпись _____	***(доверенность №_____ от «_____» _____ 20 ___ г.)*** Должность_____ Ф.И.О. _____ Подпись _____
Должность_____ Ф.И.О. _____ Подпись _____	

Дата, время передачи: «__ __»_____ 20___ г. ___ ___ _____
(час, мин.)

Руководитель Клиента: _____
(Ф.И.О.)

Подпись _____ М.П.
(при наличии)

Приложение 7
к Договору присоединения на обслуживание
в системе «Onlinebank HALYK»

СОГЛАШЕНИЕ НА ВЫДАЧУ ФАЙЛОВОГО СЕРТИФИКАТА

г. _____ «___» _____ 20__г.

Акционерное общество «Народный сберегательный банк Казахстана», именуемое в дальнейшем **«Банк»,** в лице _____, действующего на основании _____, с одной стороны и _____, именуемое в дальнейшем **«Клиент»,** в лице_____ действующего на основании _____, с другой стороны, далее совместно именуемые «**Стороны**», а отдельно как указано выше или «**Сторона**», принимая во внимание, что заключенным между Сторонами Договором присоединения на обслуживание в системе Onlinebank HALYK (далее - Договор) предусмотрена возможность использования Клиентом регистрационного свидетельства в виде электронного документа, заключили настоящее Соглашение на выдачу файлового сертификата (далее – «**Соглашение**») о нижеследующем:

1. Банк выдает каждому уполномоченному Клиентом лицу регистрационное свидетельство в виде электронного документа (далее – файловый сертификат) способом, указанным Клиентом в заявлении, без записи его на Ключевой носитель. Ключевой носитель и Pin-код к нему, Карт ридер не используются и не выдаются Клиенту.
2. Клиент безусловно соглашается с тем, что степень защиты файлового сертификата ниже, чем степень защиты регистрационных свидетельств, выданных на ключевом носителе, так как файловый сертификат защищен только паролем. Пароль известен только уполномоченному Клиентом лицу, которому выдан файловый сертификат. Все риски, связанные с возможным несанкционированным использованием файловых сертификатов, регистрируемых согласно настоящему Соглашению и используемых для подписания электронных документов Клиента, несет Клиент. Электронные документы, подписанные электронной цифровой подписью, сформированной с использованием файловых сертификатов, безусловно признаются направленными Клиентом, если до их направления Банку не было направлено сообщение о возникновении угрозы несанкционированного доступа к файловому сертификату, об аннулировании файлового сертификата или прекращении полномочий лиц, которым файловые сертификаты были выданы.
3. Клиент обязуется обеспечить использование файлового сертификата/файловых сертификатов уполномоченными им лицами, которым выданы файловые сертификаты, таким образом, чтобы ограничить доступ к ним со стороны третьих лиц. Банк не несет ответственность за ненадлежащую защиту Клиентом файлового сертификата вне зависимости от выбранного/ых Клиентом способа защиты/способов защиты.
4. Особенности использования файлового сертификата.

Для безопасности работы веб-сервисов Удостоверяющий центр выпускает защищённые паролем файловые сертификаты в формате .pfx.

Для совершения любых действий в веб-сервисе, включая скрепление документов электронной цифровой подписью, должен использоваться файловый сертификат. Для использования файлового сертификата нужно получить ключ из файла .pfx. Дополнительно необходимо получить сертификат из данного файла. Для всех данных действий существуют API в разных языках программирования.

В случае разработки «клиента» для веб-сервиса с помощью языка Java существуют два способа получения ключа:

1) Импортировать ключ и сертификат в java keystore (хранилище ключей). Чтобы импортировать ключ и сертификат из .pfx файла в keystore, необходимо использовать программы openssl и keytool;
2) Использование .pfx файла как хранилище напрямую из java-кода.

Например:

```
KeyStore pfx = KeyStore.getInstance("pkcs12");
pfx.load(new FileInputStream("somefile.pfx"), password).
```

В случае использования другого языка программирования, например, C++, при помощи двойного клика по файлу необходимо сохранить ключ в хранилище Windows, затем с помощью WinAPI получить его из хранилища в коде.

5. Передача Банком Клиенту файлового сертификата осуществляется в течение 10 (десяти) рабочих дней с момента его выпуска Удостоверяющим центром, и оформляется Актом приема-передачи файлового

сертификата, форма которого приведена в приложении 1 к настоящему Соглашению. Акт приема-передачи файлового сертификата составляется Банком в двух оригинальных экземплярах по одному для каждой Стороны, подписывается уполномоченными представителями обеих Сторон и скрепляется печатью Банка. Клиент скрепляет Акт приема-передачи файлового сертификата печатью в случае ее наличия.

6. Все термины, применяемые в настоящем Соглашении, употребляются в том значении, в каком они применяются в заключенном Сторонами Договоре.

7. При использовании уполномоченными Клиентом лицами файловых сертификатов условия Договора применяются с учетом особенностей, предусмотренных настоящим Соглашением.

Те условия Договора, которые не затрагиваются настоящим Соглашением, остаются в силе без изменений и Стороны подтверждают по ним свои обязательства.

8. Настоящее Соглашение вступает в силу с даты его заключения и является неотъемлемой частью Договора.

9. Соглашение составлено в двух подлинных экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

«Банк»	**«Клиент»**
АО «Народный Банк Казахстана»	
Адрес Банка: _____ БИК: HSBKKZKX БИН: 940140000385	Юридический адрес: _____ тел/факс_____ БИН (ИИН): _____ ИИК _____
От Банка Должность: _____ Ф.И.О. _____ Подпись _____ М.П. (при наличии)	От Клиента Должность: _____ Ф.И.О. _____ Подпись _____ М.П. (при наличии)

Приложение 1
к Соглашению на выдачу файлового сертификата

АКТ ПРИЕМА-ПЕРЕДАЧИ
файлового сертификата

«_ __» ___ _____ 20__ _г.

Мы, нижеподписавшиеся, подтверждаем передачу файлового сертификата в соответствии с условиями Соглашения.

Наименование Клиента: _____

БИН/ИИН: _____

Данные уполномоченного лица:

Фамилия _____

Имя _____

Отчество (при наличии) _____ _____

ИИН _____

Серийный номер: ___ _____

Передал:	**Принял:**
От Банка	От Клиента
Должность_____ Ф.И.О. _____ Подпись _____ ___	***(доверенность №_____ от «_____» _____ _ 20 ___ г.)*** Должность_____ Ф.И.О. _____ Подпись _____

Дата, время передачи: «_____»_____ 20____ г. _____ _____
(час, мин.)

Руководитель Клиента: _____
(Ф.И.О.)

Подпись _____ М.П.
(при наличии)