Кому:
БИН:

От: Товарищества с ограниченной ответственностью «DauInvest»
БИН: 191240020942

Исх.№_____ от __.__.2026 года

О сервисе «TrustContract»

В рамках формирования экосистемы цифрового доверия «TrustMe» Товарищество с ограниченной ответственностью «DauInvest» разработало и ввело в коммерческую эксплуатацию сервис **«TrustContract»**, платформу для заключения, подписания и хранения договоров и иных юридически значимых документов в электронной форме. Сервис предоставляет четыре самостоятельных способа подтверждения при подписании документов: (1) подтверждение волеизъявления посредством одноразового SMS-кода; (2) биометрическая верификация личности; (3) подписание через мобильное приложение egov mobile с использованием облачного цифрового ключа; (4) через ЭЦП. Каждый из способов является отдельным, независимым правовым инструментом.

По состоянию на дату выдачи настоящей справки сервисом «TrustContract» пользуются более 1,5 миллиона физических и более 10 000 юридических лиц из Казахстана и иностранных государств, что свидетельствует о его практической востребованности и фактическом признании участниками гражданского оборота.

Настоящая справка подготовлена в целях подтверждения законности всех трех применяемых в сервисе «TrustContract» способов подписания документов и обоснования их соответствия действующему законодательству Республики Казахстан, включая **Цифровой кодекс Республики Казахстан № 255-VIII**, принятый 9 января 2026 года и вводимый в действие с 11 июля 2026 года.

Правовые основания законности подписания документов через сервис «TrustContract»

1. Гражданское законодательство Республики Казахстан

Согласно статье 151 Гражданского кодекса Республики Казахстан согласие на совершение сделки либо на оформление любого документа может выражаться не только проставлением подписи и печати или подписанием посредством ключа электронной цифровой подписи (далее – ЭЦП), но и иным способом выражения своего согласия для совершения определенных действий. Данная норма является основополагающей: закон намеренно не ограничивает допустимые формы волеизъявления и допускает широкий спектр способов его выражения.

В соответствии с пунктом 3 статьи 152 Гражданского кодекса Республики Казахстан для придания сделке или документу полной юридической силы необходимо соблюдение двух ключевых требований: (1) надлежащее определение субъектов (сторон) документа и (2) наличие и фиксация их волеизъявления. Письменная форма документа при этом прямо не ограничивается бумажным носителем – законодатель допускает электронную, цифровую и иные формы при соблюдении указанных требований.

Таким образом, с точки зрения Гражданского кодекса РК, подписание документа в сервисе «TrustContract» посредством SMS-кода является допустимой формой выражения волеизъявления при условии надлежащей идентификации стороны – что обеспечивается описанными ниже механизмами.

2. **Цифровой кодекс Республики Казахстан: цифровое подтверждение как самостоятельный правовой инструмент**

Цифровой кодекс Республики Казахстан № 255-VIII (далее – Цифровой кодекс РК) на уровне кодифицированного акта закрепляет два самостоятельных и равнозначно

признаваемых инструмента выражения волеизъявления в цифровой среде: **электронную цифровую подпись (ЭЦП)** и **цифровое подтверждение (в том числе SMS-код и биометрию).** Законодатель прямо признает, что ЭЦП является лишь одним из возможных способов волеизъявления в цифровой среде, но не единственным. SMS-подтверждение и биометрическая аутентификация при этом являются ***отдельными, независимыми друг от друга*** механизмами, каждый из которых обладает самостоятельной правовой силой.

2.1. **Подписание документов посредством SMS-кода**

Согласно ст. 47 Цифрового кодекса РК, цифровое подтверждение определяется как «действие субъекта цифровой среды, выражающее согласие или иное волеизъявление, совершаемое после прохождения цифровой аутентификации с использованием средств цифровых технологий». К цифровым подтверждениям прямо отнесены коды, пароли, одноразовые цифровые идентификаторы, пуш-уведомления и иные средства, направляемые на абонентские устройства сотовой связи, сервисы мгновенных сообщений, электронную почту, а также распределенные цифровые объекты.

SMS-код, применяемый в сервисе «TrustContract», по своей правовой природе является одноразовым цифровым идентификатором, направляемым на абонентское устройство сотовой связи, что прямо предусмотрено статьей 47 Цифрового кодекса РК. Механизм подписания документов посредством SMS-кода **полностью укладывается в легальное определение цифрового подтверждения**.

Статья 5 Цифрового кодекса РК – свободное и осознанное волеизъявление:

Статья 5 Цифрового кодекса РК закрепляет принцип: **«*отношения в цифровой среде основываются на свободном, осознанном и выраженном волеизъявлении человека*».** Подтверждение документа посредством SMS-кода полностью отвечает данному принципу: сторона совершает активное, осознанное действие – вводит одноразовый код, полученный лично ею на зарегистрированный номер, тем самым ясно и недвусмысленно выражая свое согласие с содержанием документа.

Статья 46 Цифрового кодекса РК – цифровая аутентификация:

Цифровая аутентификация определяется как **«*процедура подтверждения личности физического лица или правоспособности юридического лица при доступе к услугам в цифровой среде*».** В сервисе «TrustContract» цифровая аутентификация при SMS-подписании осуществляется посредством верификации абонентского номера сотовой связи, зарегистрированного на конкретное лицо по ИИН/БИН, что придает подписанным документам доказательную силу в правоотношениях.

Принцип технологической нейтральности (статья 12 Цифрового кодекса РК):

Статья 12 Цифрового кодекса РК закрепляет **принцип технологической нейтральности** правового регулирования, предполагающий равное отношение к различным цифровым технологиям исходя из их функциональных характеристик. Данный принцип подтверждает, что SMS-подтверждение и ЭЦП как функционально равнозначные инструменты выражения волеизъявления не должны иметь различного правового режима при одинаковом результате – установлении сторон и их согласия.

2.2. **Идентификация сторон при SMS-подписании**

Действия, совершенные с использованием мобильного устройства, или любого другого устройства, имеющего SIM-карту, являются действиями абонента, на которого SIM-карта оформлена (т.е. документ, подписанный СМС–кодом позволяет идентифицировать стороны), **соответственно подписав документ посредством одноразового СМС-кода можно определить и установить факт его совершения, идентифицировать стороны документа и определить содержание их волеизъявления.**

В соответствии с п.67-2) Закона Республики Казахстан от 5 июля 2004 года N 567 «О связи», **база данных идентификационных кодов абонентских устройств сотовой**

связи – аппаратно-программный комплекс управления базой данных, содержащей сведения об:

индивидуальных идентификационных номерах (для физических лиц) или бизнес-идентификационных номерах (для юридических лиц) владельцев абонентских устройств сотовой связи;

идентификационных кодах абонентских устройств сотовой связи;

абонентских номерах, используемых абонентскими устройствами сотовой связи.

Соответственно, для регистрации абонентских устройств сотовой связи была запущена в эксплуатацию база данных идентификационных кодов (БДИК), в которой регистрация абонентов операторами связи осуществляется по схеме «IMEI код + номер SIM карты + ИНН/БИН абонента».

Так, в соответствии с вышеуказанными требованиями услуги сотовой связи не оказываются незарегистрированным абонентам, ввиду того что IMEI сотового устройства, использующего SIM-карту, должен числиться за ИИН/БИН владельцем (т.е. зарегистрированным пользователем). Каждый абонентский номер однозначно привязан к конкретному лицу, что **позволяет достоверно установить подписанта по номеру, на который направлен SMS-код**.

Интеграция с государственными базами данных (ГБД ФЛ, ГБД ЮЛ и БМГ). Сервис «TrustContract» располагает интеграцией с тремя государственными базами данных, которые в совокупности образуют многоуровневый механизм идентификации подписывающего лица и существенно усиливают надежность способа подписания через ПЭП:

Государственная база данных «Физические лица» (ГБД ФЛ) – содержит актуальные регистрационные сведения о каждом физическом лице, зарегистрированном в Республике Казахстан: полное имя, ИИН, дату рождения, паспортные данные. Интеграция с ГБД ФЛ позволяет сервису «TrustContract» в режиме реального времени верифицировать личность подписывающего физического лица и подтвердить актуальность его регистрационных данных на момент подписания документа. Тем самым ГБД ФЛ **четко и однозначно устанавливает личность подписанта**, исключая возможность подписания документа от имени несуществующего или неверно идентифицированного лица.

Государственная база данных «Юридические лица» (ГБД ЮЛ) – содержит сведения о зарегистрированных юридических лицах и индивидуальных предпринимателях: наименование, БИН, юридический адрес, сведения о руководителях и уполномоченных представителях. Интеграция с ГБД ЮЛ позволяет верифицировать правоспособность юридического лица, полномочия его представителя на момент подписания, а также подтвердить корпоративную принадлежность подписывающего лица. ГБД ЮЛ **устраняет риск подписания документа неуполномоченным лицом** или представителем ликвидированной (реорганизованной) организации, что особенно критично при заключении договоров между организациями.

База мобильных граждан (БМГ) – государственный реестр, связывающий абонентский номер сотовой связи с ИИН его владельца. Интеграция с БМГ обеспечивает критически важное звено идентификационной цепочки при SMS-подписании: система устанавливает, что номер телефона, на который направлен одноразовый SMS-код, **официально зарегистрирован именно за тем лицом, которое является стороной подписываемого документа**. Это исключает ситуацию, при которой SMS-код мог бы быть направлен на номер, не принадлежащий подписывающему лицу. БМГ тем самым формирует неразрывную цифровую связь между подписантом и использованным средством волеизъявления.

Таким образом, совокупная интеграция сервиса «TrustContract» с ГБД ФЛ, ГБД ЮЛ и БМГ создает **многоуровневую государственную верификацию подписывающего лица**: (1) подтверждение личности физического лица через ГБД ФЛ; (2) подтверждение

правоспособности и полномочий представителя юридического лица через ГБД ЮЛ; (3) установление принадлежности абонентского номера конкретному лицу через БМГ. Данный механизм полностью удовлетворяет требованиям пункта 3 статьи 152 Гражданского кодекса РК о надлежащем определении субъектов документа и обеспечивает значительно более высокий уровень идентификации, чем при традиционном бумажном подписании.

Идентификация при SMS-подписании обеспечивается совокупностью: (1) регистрационных данных пользователя; (2) привязки номера телефона к ИИН/БИН через БМГ; (3) верификации личности и правоспособности через ГБД ФЛ/ГБД ЮЛ; (4) направления одноразового SMS-кода на зарегистрированный номер конкретного лица.

2.3. **Подписание документов посредством биометрической аутентификации**

Статья 48 Цифрового кодекса РК – биометрическая аутентификация:

Биометрическая аутентификация – прямо предусмотренный статьей 48 Цифрового кодекса РК самостоятельный способ подтверждения личности, определяемый как «процесс сравнения и проверки соответствия биометрических данных для цели установления личности».

Биометрическая аутентификация в сервисе «TrustContract» является самостоятельным, независимым от иных способов механизмом подписания документов. Стороны вправе применять ее отдельно как полноценный, юридически значимый способ выражения волеизъявления.

Статья 47 Цифрового кодекса РК – биометрия как вид цифрового подтверждения:

Указанная статья прямо включает «биометрические подтверждения» в перечень цифровых подтверждений – форм выражения согласия или иного волеизъявления в цифровой среде. Таким образом, биометрическая аутентификация одновременно является как самостоятельным способом установления личности (статья 48), так и полноправной формой цифрового подтверждения волеизъявления (статья 47).

Статьи 5 и 46 Цифрового кодекса РК:

Прохождение биометрической аутентификации – **сознательное, активное действие стороны**, совершаемое исключительно при ее личном участии, что в полной мере отвечает принципу «свободного, осознанного и выраженного волеизъявления» (статья 5). Биометрическая верификация представляет собой цифровую аутентификацию в смысле статьи 46 Цифрового кодекса РК и является «основанием для возникновения, изменения или прекращения правоотношений в цифровой среде, а также для целей доказывания юридически значимых действий».

2.4. **Идентификация сторон при биометрической аутентификации**

Биометрические данные как персональные данные. Биометрические данные являются персональными данными конкретного физического лица и однозначно его идентифицируют. Сравнение биометрических данных с эталонным образцом позволяет с высокой степенью достоверности установить личность подписанта.

Идентификация при биометрическом подписании обеспечивается: (1) регистрационными данными пользователя; (2) уникальными биометрическими характеристиками лица. Биометрическая идентификация является **наиболее достоверным способом установления личности**, поскольку неразрывно связана с конкретным физическим лицом и не может быть делегирована третьему лицу без его ведома.

2.5. **Подписание документов через приложение egov mobile**

Мобильное приложение egov mobile является официальным государственным цифровым объектом «цифрового правительства» Республики Казахстан, посредством которого физические и юридические лица получают доступ к государственным услугам и осуществляют юридически значимые действия в цифровой среде.

Для входа в egov mobile пользователь **проходит аутентификацию с использованием облачного цифрового ключа** (облачной ЭЦП) – закрытого ключа электронной цифровой подписи, хранящегося в защищенном облачном хранилище Национального удостоверяющего центра Республики Казахстан (НУЦ РК) и доступного пользователю через мобильное приложение без необходимости хранения ключа на физическом носителе. После успешной аутентификации пользователь вправе подписать направленный ему документ непосредственно в приложении egov mobile, используя облачную ЭЦП, что **порождает полноценный электронный документ в смысле Цифрового кодекса РК**.

3. Хранение документов в блокчейне: гарантия неизменности

Сервис «TrustContract» обеспечивает хранение всех подписанных документов в распределенном реестре (блокчейне), что полностью соответствует положениям Цифрового кодекса РК.

Статья 26 Цифрового кодекса прямо признает **распределенные цифровые объекты** как цифровые объекты, создание, хранение и обработка которых осуществляются посредством распределенной архитектуры, обеспечивающей согласованность, достоверность и целостность цифровых записей без единого центра их обработки. Это и есть принцип работы блокчейна.

Функционирование распределенных цифровых объектов основывается на внутреннем регламенте взаимодействия, определяющем **алгоритмы обеспечения согласованности, достоверности и неизменности цифровых записей** (ст. 26 ЦК РК). Запись в блокчейне криптографически защищена от последующего изменения, что обеспечивает:

- **неизменность документа** – после фиксации в блокчейне содержание документа не может быть изменено ни одной из сторон;
- **верифицируемость** – любая сторона или суд может в любой момент проверить подлинность записи по хешу транзакции;
- **временную метку** – фиксируется точное время подписания, подтверждающем момент существования подписи;
- **децентрализованное хранение** – исключается риск утраты документа вследствие технического сбоя на стороне одного из участников.

Таким образом, хранение документов в блокчейне в рамках сервиса «TrustContract» представляет собой правомерно применяемый распределенный цифровой объект по смыслу ст. 26 Цифрового кодекса РК, обеспечивающий более высокий уровень доказательной силы документа по сравнению с традиционными способами хранения.

4. Аналогичные механизмы, применяемые в Республике Казахстан

Все три механизма уже широко и правомерно применяются в Казахстане в сферах, где юридическая значимость действий пользователей не вызывает сомнений:

- **Портал egov.kz и приложение egov mobile** – подписание заявлений и получение государственных услуг осуществляются через SMS-код и облачную ЭЦП. Данные механизмы являются официально признанными государством инструментами волеизъявления граждан.
- **Банковский сектор** (Kaspi.kz, Halyk Bank, ForteBank и другие) – оформление кредитных договоров и финансовых операций осуществляется через SMS-подтверждение и биометрическую верификацию. Данная практика прямо допущена регулятором финансового рынка.

- **Платежные системы и страхование** – заключение договоров страхования и оформление платежных поручений сопровождается SMS-верификацией, биометрией и подписанием посредством ЭЦП.
- **Мировые лидеры рынка электронного подписания** – DocuSign, Adobe Sign и другие – успешно и правомерно работают в десятках государств, в том числе с развитой правовой системой (США, ЕС, ОАЭ). Их деятельность основана именно на ПЭП-механизмах: нажатие кнопки «Подписать», ввод SMS-кода, подтверждение в приложении.

Перечисленные аналоги свидетельствуют о том, что все три механизма являются признанными стандартами волеизъявления в казахстанской цифровой среде, а с вступлением в силу Цифрового кодекса РК они получают прямое законодательное закрепление.

5. Типовой закон ЮНСИТРАЛ об электронных подписях: принцип технологической нейтральности на международном уровне

Правовая позиция ТОО «DauInvest» в отношении допустимости ПЭП находит подтверждение не только в казахстанском законодательстве, но и на уровне международного права. Комиссия ООН по праву международной торговли (ЮНСИТРАЛ) разработала **Типовой закон ЮНСИТРАЛ об электронных подписях (2001 год)**, принятый резолюцией Генеральной Ассамблеи ООН № 56/80. В основу этого документа положен фундаментальный принцип: ни одному методу электронного подписания не может быть отказано в юридической силе исключительно по причине используемой технологии. Данный принцип является системообразующим для всего мирового регулирования электронных подписей и непосредственно влияет на оценку допустимости ПЭП.

Статья 3 Типового закона ЮНСИТРАЛ – равный режим для всех технологий электронного подписания. Данная статья закрепляет основополагающий принцип, согласно которому не допускается дискриминация в отношении ни одного из способов электронного подписания: все технологии подписания должны иметь равные возможности для получения правового признания при условии выполнения ими функций, эквивалентных собственноручной подписи. Согласно руководству по принятию Типового закона (пункт 107), форма применения определенных электронных подписей **не может использоваться в качестве единственного основания для отказа в их юридической силе**.

Признание широкого спектра технологий подписания. В руководстве по принятию Типового закона ЮНСИТРАЛ (пункт 82) прямо перечислены технологии, которые подпадают под режим технологической нейтральности: цифровые подписи на основе асимметричной криптографии, биометрические устройства (идентификация по геометрии лица, отпечаткам пальцев, распознаванию голоса, сканированию сетчатки глаза), персональные идентификационные номера (ПИН), одноразовые цифровые идентификаторы, нажатие кнопки подтверждения («ОК»). Таким образом, международный документ ООН прямо признает SMS-коды (одноразовые идентификаторы), биометрию и иные ПЭП-механизмы законными формами электронного подписания наряду с криптографической ЭЦП, не устанавливая между ними какой-либо иерархии по юридической силе.

Функциональный эквивалент как критерий признания. Типовой закон ЮНСИТРАЛ основывается на подходе «функционального эквивалента»: любой метод подписания признается правомерным, если он выполняет те же функции, что и собственноручная подпись, идентификацию лица и фиксацию его волеизъявления. SMS-код, направляемый на абонентский номер, зарегистрированный за конкретным лицом, и биометрическая аутентификация в полной мере выполняют обе эти функции: идентифицируют подписанта и фиксируют его осознанное волеизъявление.

Принцип технологической нейтральности, закрепленный в статье 3 Типового закона ЮНСИТРАЛ, нашел свое прямое воплощение в казахстанском законодательстве: статья 12 Цифрового кодекса РК воспроизводит этот же принцип, устанавливая равное отношение ко всем цифровым технологиям исходя из их функциональных характеристик. Таким образом, подход казахстанского законодателя полностью согласуется с международными стандартами ООН в данной области.

6. **Возможность подписания с использованием ЭЦП для клиентов, предпочитающих усиленную электронную подпись**

Несмотря на полную законность и достаточность ПЭП-механизмов (SMS-код, биометрия, egov mobile) для целей подписания документов в сервисе «TrustContract», ТОО «DauInvest» понимает, что часть клиентов может испытывать сомнения в юридической достаточности простой электронной подписи или предпочитать максимально высокий уровень криптографической защиты документа. Для таких клиентов сервис «TrustContract» предоставляет полноценную возможность подписания документов с использованием **электронной цифровой подписи (ЭЦП)**, выданной Национальным удостоверяющим центром Республики Казахстан (НУЦ РК).

ЭЦП, применяемая в сервисе «TrustContract», полностью соответствует требованиям Цифрового кодекса РК, выдается аккредитованным удостоверяющим центром (НУЦ РК) и обеспечивает криптографическую защиту подписанного документа. При подписании ЭЦП в документ вносится уникальная цифровая метка, неразрывно связанная с его содержанием, что исключает любое последующее изменение документа без нарушения целостности подписи. Таким образом, клиенты сервиса «TrustContract» могут выбрать способ подписания, соответствующий их уровню требований к юридической защищенности документа: от удобного ПЭП для повседневных операций до ЭЦП для документов, в отношении которых желательна максимальная криптографическая защита.

7. **Заключение**

На основании изложенного ТОО «DauInvest» настоящим подтверждает, что **подписание документов в электронной форме посредством сервиса «TrustContract»** через SMS-подтверждение, биометрическую аутентификацию или приложение egov mobile – является **полностью законным** и соответствует законодательству Республики Казахстан

С уважением,
CEO of TrustContract
ТОО «DauInvest»
Мансурова Д.Х.

М.П.