

Договор № _____
по обслуживанию банковского счета с использованием
программного комплекса “Банк-Клиент”

г. Ташкент

“ ___ ” _____ 200_ г.

Банк “Асака” (ОАО), именуемый в дальнейшем “Банк”, в лице _____,
действующего на основании _____,
с одной стороны, и _____, именуемый в дальнейшем
“Клиент”, в лице _____,
действующего на основании _____, с другой стороны,
вместе именуемые “Стороны”, заключили настоящий Договор о нижеследующем:

1. Предмет Договора

1.1. Банк представляет Клиенту услуги по выполнению расчетов с использованием денежно-расчетных документов в электронной форме посредством программного комплекса “Банк-Клиент” (ПК “Банк-Клиент”), обеспечивающего подготовку электронных денежно-расчетных документов, формирование запросов и сообщений, шифрование информации и электронную подпись, модемную связь с Банком, прием-передачу информации, обработку полученной информации, печать выходных форм, архивирование информации. При осуществлении расчетов по системе ПК “Банк-Клиент” Клиент перечисляет средства со своего счета только в форме платежного поручения.

1.2. Услуги Клиенту оказываются Банком посредством программного комплекса, устанавливаемого Банком в офисе на оборудование Клиента. Инсталляция и запуск ПК “Банк-Клиент”, а также обучение Клиента работе оформляются двухсторонним актом сдачи комплекса в эксплуатацию.

1.3. Банк и Клиент признают метод шифрования информации и электронную подпись, используемые в ПК “Банк-Клиент”.

1.4. Клиент доверяет Банку передачу в Центральный банк Республики Узбекистан поступивших по каналам связи электронных денежно-расчетных документов до получения оригиналов. Полученные Банком электронные денежно-расчетные документы признаются правомочными и обязательными к исполнению и хранятся вместе с полученными впоследствии оригиналами.

1.5. В случае возникновения у Банка или Клиента каких-либо обстоятельств, препятствующих обмену электронными документами, представление Клиентом соответствующих документов на бумажном носителе производится в порядке, предусмотренном Договором банковского счета.

1.6. Настоящий договор является неотъемлемой частью Договора банковского счета № _____ от “ ___ ” _____ 200_ г., заключенного между Сторонами.

1.7. Оплата за услуги производится согласно «Тарифам комиссионного вознаграждения за выполнение поручений клиентов».

2. Обязанности Банка

2.1. Банк обязуется в течение 15 дней после подачи заявки Клиентом о его технической готовности к подключению системы:

- установить программное обеспечение, необходимое для работы ПК “Банк-Клиент”.
- обеспечивать идентификацию владельца счета и проверку подлинности полученных от него электронных документов по цифровой электронной подписи КЛИЕНТА, порядок вычисления которой под документами изложен в Приложении 1А к настоящему Договору, а также по факту декодирования сообщений клиента с помощью его зарегистрированного открытого ключа (см. Приложение 1Б);
- вести регистрацию полученных и переданных электронных документов в журнале учета;
- обучить персонал работе с ПК “Банк-Клиент”.

2.2. Прием электронных денежно-расчетных документов от Клиента производится Банком в рабочие дни:

- по исходящим платежам в другие банки - с 9.00 до 14.00;
- по исходящим платежам внутри банка - с 9.00 до 15.00.

Банк обязуется проводить электронные денежно-расчетные документы, полученные в указанное время, в день их получения. Документы, поступившие после указанного времени, Банком не исполняются.

2.3. Электронные платежные денежно-расчетные документы принимаются Банком к исполнению только при оформлении их в соответствии с требованиями п. 3.7. данного договора и наличии электронных подписей распорядителей кредита Клиента.

2.4. Банк обязуется немедленно закрыть прием электронных документов с электронной подписью Клиента и информировать его при угрозе несанкционированного доступа к его счетам до выяснения обстоятельств происшедшего. Восстановление работы комплекса возможно только по согласованию с Клиентом и после замены электронных подписей и ключей шифрования.

2.5. Банк обязан не принимать к исполнению денежно-расчетные документы, поступившие от Клиента в электронном виде, при отсутствии электронной подписи файла или ее некорректности и направить Клиенту отказ в электронном виде от приема такого документа с указанием причины.

2.6. Банк обязан не принимать к исполнению электронные денежно-расчетные документы, выполненные с отступлением от форматов, реализованных в поставляемых Банком Клиенту программных средствах ввода и криптографии платежных документов.

2.7. Банк обязан направлять Клиенту извещение о приеме файла с электронными документами, заверенное электронной подписью. Время, указанное в извещении, является временем приема документа. При возникновении расхождения по времени приема документа Стороны признают, что определяющим временем является текущее время по системным часам аппаратных средств Банка.

2.8. Банк не несет ответственности за ущерб, возникший вследствие предоставления доступа к комплексу, передачи паролей и электронных подписей

третьим лицам, неправильного лицам, неправильного оформления Клиентом электронных денежно-расчетных документов.

2.9. В случае потери работоспособности программного обеспечения клиентской части системы (находящейся на машине Клиента), возникшей не по вине Клиента, Банк обязуется в течении 5 (пяти) рабочих дней после подачи Клиентом заявки об этом в Банк восстановить нормальную работоспособность клиентской части системы.

3. Обязанности Клиента

3.1. Для работы с ПК “Банк Клиент” Клиент использует собственное техническое оборудование в следующей комплектации:

- персональный компьютер с соответствующим системным обеспечением;
- модем;
- печатающее устройство;
- телефакс

3.2. Регистрация, в случае необходимости, установленного коммуникационного оборудования или другой используемой системы связи возлагается на Клиента.

3.3. Клиент обязуется содержать компьютер, на котором установлен ПК “Банк-Клиент”, в охраняемом опечатываемом служебном помещении, доступ в которое разрешен только сотрудникам, непосредственно работающим с ПК “Банк-Клиент”, не производить изменения в конфигурации компьютера и операционной системы без письменного согласования с администратором ПК «Банк-Клиент» Банка «Асака».

3.4. Обеспечивать сохранность и защиту от использования не по назначению ключевых элементов для цифровой электронной подписи и защиты передаваемых в БАНК сообщений.

3.5. Обеспечить использование каждой программы цифровой электронной подписи только уполномоченными на распоряжение счетом КЛИЕНТА лицами.

3.6. Клиент не имеет права тиражировать (в целях резервного копирования и т.д.) программное обеспечение, поставляемое банком. За нарушение настоящего требования Клиент несет ответственность в порядке, предусмотренном действующим законодательством. При использовании нескольких копий программного обеспечения банк не несет ответственности за дальнейшую работоспособность системы и возможные убытки Клиента, образованные вследствие этого.

3.7. При утере криптографического ключа и в других случаях возникновения угрозы несанкционированного доступа к компьютеру, Клиент немедленно ставит в известность Банк. Восстановление работы комплекса возможно только после замены криптографических ключей и паролей Клиента.

3.8. Клиент имеет право в любой момент времени потребовать замены ключей кодирования и паролей.

3.9. Клиент обязан заполнять документы в соответствии с действующим законодательством Республики Узбекистан.

3.10. Клиент может получать за каждый операционный день заверенные электронной подписью Банка выписки в электронном виде и контролировать

движение средств по своим счетам путем проверки данных в выписках и оригиналах платежных документов. При невозможности получения выписок или несоответствии данных выписок оригиналам платежных документов Клиент обязан немедленно известить об этом Банк любым доступным способом.

4. Стороны обязуются

4.1. Обеспечивать сохранение в тайне сведений по вопросам технологии системы электронных платежей между Сторонами за исключением случаев, предусмотренных действующим законодательством.

4.2. При выявлении признаков или фактов нарушения безопасности системы одной из Сторон немедленно приостановить расчеты по ПК “Банк-Клиент” и известить другую Сторону для принятия соответствующих мер.

4.3. Формировать и поддерживать архивы всех принятых и переданных электронных документов с цифровыми подписями. Срок поддержания архива - 10 лет, а в случае возникновения споров - до их разрешения. Стороны несут ответственность за целостность и достоверность своих электронных архивов.

4.4. Соблюдать все правила безопасности и технической защиты информации. Организовать внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность использования системы другими лицами, не имеющими допуска работы с ней, а также исключить возможность использования электронной подписи лицами, не имеющими права подписи финансовых документов.

5. Ответственность сторон

5.1. За нарушение принятых по настоящему Договору обязательств стороны несут ответственность в соответствии с действующим законодательством

5.2. Клиент несет ответственность за сохранность средств криптографии, правильность формирования электронных документов, шифрацию и передачу их в Банк по каналам связи.

5.3. Информация, оформленная Стороной на бумажном носителе, преобразуется в электронный документ, при этом вся ответственность за соответствие бумажного документа созданному на его основе электронному документу полностью возлагается на Сторону, создавшую электронный документ.

5.4. Несоблюдение Клиентом обязательств, предусмотренных разделом 3 настоящего договора, влечет за собой ответственность, как перед Банком, так и перед третьими лицами.

6. Форс-мажор

6.1. В случае возникновения форс-мажорных обстоятельств, а также других обстоятельств, не зависящих от воли сторон, стороны приостанавливают обмен финансовыми документами на все время действия форс-мажорных обстоятельств и обязуются в разумно короткий срок с момента наступления таких обстоятельств уведомить друг друга об их наступлении любым возможным видом связи.

6.2. Банк не несет ответственности перед Клиентом за прекращение использования системы, возникшее вследствие действия непреодолимой силы, существенно влияющей на функционирование системы электронных платежей, в виде стихийных бедствий, как наводнение, пожар, землетрясение и другие стихийные бедствия, эмбарго, военные действия, отключения электроэнергии, повреждения линии связи, общественных явлений, а также решений органов власти, принимаемых в центре и на месте, и обязательных для исполнения Банком.

7. Порядок разрешения споров

7.1. При возникновении разногласий и споров, связанных с исполнением Сторонами настоящего Договора, Стороны обязуются решать их путем переговоров. На время разрешения спорной ситуации, связанной с исполнением Банком поручения Клиента, Банк имеет право приостановить действие настоящего Договора в одностороннем порядке с последующим уведомлением Клиента.

7.2. Стороны соглашаются следовать процедуре разрешения споров по электронным документам с цифровой подписью (см. Приложение 2), которая является неотъемлемой частью настоящего Договора.

7.3. Споры будут рассматриваться только на основании электронных платежных документов в том виде, в каком они поступили по каналам связи.

7.4. Если одна из Сторон предъявляет другой Стороне претензию по документу, а также подтверждение другой Стороны о получении такого документа, а другая Сторона не может представить архивную копию спорного документа вследствие ненадлежащего хранения архива виновной признается Сторона, не представившая архивную копию спорного документа.

7.5. Споры, по которым не достигнуто соглашение Сторон, разрешаются в Хозяйственном суде.

8. Срок действия Договора и порядок его расторжения

8.1. Настоящий договор вступает в силу с даты его подписания и считается заключенным на неопределенный срок.

8.2. Любая из сторон имеет право расторгнуть настоящий Договор в одностороннем порядке досрочно, предупредив другую сторону не менее чем за один месяц до предполагаемой даты расторжения.

8.3. При расторжении Договора стороны обязаны выполнить все взаимные обязательства, вытекающие из настоящего Договора и всех дополнительных соглашений Сторон к настоящему Договору. При этом Клиент обязан предоставить Банку возможность удаления клиентской части комплекса.

8.4. Расторжение настоящего Договора не влечет за собой расторжения Договора банковского счета. Расторжение Договора банковского счета влечет за собой расторжение настоящего Договора.

9. Прочие условия

9.1. В случае необходимости внесения изменений либо дополнений в установленный ПК “Банк-Клиент”, настоящий Договор по взаимному согласию Сторон может быть изменен или дополнен приложениями к нему.

9.2. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу. Один экземпляр - для Банка, другой - для Клиента.

9.3 Приложения 1А, 1Б и 2 являются неотъемлемой частью настоящего Договора.

10. Юридические адреса сторон

Банк: _____

Клиент _____

За Банк

За Клиента

Согласовано:

Начальник юридического управления

ПОРЯДОК ПОДПИСАНИЯ И ПРОВЕРКИ ЦИФРОВОЙ ПОДПИСИ

1. Инсталляция программы подписи и подготовка ее к использованию.
 - 1.1. Все библиотеки программ фирмы “ЛАН Крипто” содержат модуль генерации ключей для подписания и проверки подписи. Получив инсталляционный комплект от фирмы “ЛАН Крипто” или представителя Банка, Клиент самостоятельно генерирует секретный и открытый ключи.
 - 1.2. Затем следует настроить подпись на владельца, то есть прописать в файл с ключом или исполняемым модулем подписания фамилию лица, которое будет подписывать документы (а также, возможно, его должность и организацию). Программа, предназначенная для этой операции, содержится в инсталляционном комплекте.
 - 1.3. Файл с секретным ключом Клиента является его единственным идентификатором, так что утеря его даже на непродолжительное время означает компрометацию ключа. Поэтому сразу после генерации необходимо принять следующие меры предосторожности:
 - 1.3.1. Файл с секретным ключом должен быть привязан к какому-либо материальному носителю, имеющему относительно небольшие размеры (что позволит носить его с собой или запирать в сейф). “ЛАН Крипто” предлагает средства привязки к двум видам таких носителей: гибкому магнитному диску (содержащему либо сам файл с ключом, либо не копируемую метку, к которой привязывается исполняемый модуль подписания) и таблетке Touch Memoгу (на которую заносится часть секретного ключа).
 - 1.3.2. На случай возможного хищения вышеупомянутого носителя рекомендуется также защитить ключ паролем.
 - 1.4. Сгенерировав ключи и настроив подпись, Клиент отправляет свой открытый ключ на носители и распечатку открытого ключа заверенную подписью и печатью в банк для регистрации. Получив в свою очередь открытый ключ банка, он тоже регистрирует его, т. е. заносит в каталог открытых ключей с помощью специальной программы.
 - 1.5. В случае, если Клиент самостоятельно не сможет генерировать свой секретный и открытые ключи, то Клиент заключает с Банком дополнительный договор о том, что он поручает Банку генерацию своих секретных и открытых ключей. В Банке создается комиссия и в присутствии комиссии клиенту генерируются секретные и открытые ключи на носителе. Клиент расписывается в специально заведенном журнале о получении секретного ключа. Открытый ключ распечатывается, заверяется подписью и печатью клиента и передается Банку для регистрации.
2. Использование программ подписи и проверки.
 - 2.1. Для подписания файла, содержащего документ, следует запустить программу подписания с обязательным параметром - именем файла. Кроме того, можно указать и необязательные параметры - опции программы подписания. Ознакомиться со значениями этих опций можно, запустив программу подписания без параметров.
 - 2.2. Если секретный ключ защищен паролем или привязкой к материальному носителю, то перед подписанием будут выданы соответствующие запросы. Необходимо ввести пароль и подключить носитель, после чего программа продолжит работу.
 - 2.3. Если значения опций, принятые по умолчанию, не удовлетворяют пользователя, их можно переопределить при помощи конфигурационного файла.
 - 2.4. В качестве обязательного параметра можно указать не имя одного файла, а маску группы файлов.

ПОРЯДОК КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ДОКУМЕНТОВ

1. Установка программы кодирования и подготовка ее к использованию.
 - 1.1. В случае, если установочный комплект содержит специальную программу установки, Клиент должен запустить эту программу и по ее запросам ввести все необходимые параметры.
 - 1.2. Следует помнить, что программа установки является одноразовой, то есть введенные параметры не могут быть изменены впоследствии. Поэтому использовать ее следует аккуратно, предварительно прочитав руководство пользователя.
 - 1.3. Библиотека программ содержит модуль генерации ключей. Получив установочный комплект непосредственно от фирмы “ЛАН Крипто” или от представителя Банка, Клиент самостоятельно генерирует индивидуальный (секретный) и общедоступный (открытый) ключи с его помощью.
 - 1.4. Файл с индивидуальным ключом Клиента требует сохранения его в секрете от всех, кроме самого хозяина, так как он ни в коем случае не должен быть скопирован посторонними лицами, что означало бы компрометацию ключа.
 - 1.5. Поэтому необходимы те же меры предосторожности, что и при использовании программ цифровой подписи, т. е. привязка к материальному носителю (дискете или таблетке Touch Memo), возможна (и желательна) защита ключа при помощи пароля.
 - 1.6. Все необходимые для этого средства имеются в установочном пакете “ЛАН Крипто”.
 - 1.7. После этого Клиент проводит те же мероприятия по обмену ключами с Банком, что и для цифровой подписи (см. Приложение 1А).
2. Использование программы кодирования.
 - 2.1. Для кодирования файла следует запустить программу кодирования с двумя обязательными параметрами: именем файла, идентификатором абонента (серийным номером или коротким именем).
 - 2.2. Как и у программы подписи, здесь имеются опции, значения которых можно увидеть, запустив программу кодирования без параметров.
 - 2.3. Можно установить их при помощи конфигурационных файлов.
 - 2.4. Поскольку секретный ключ или его часть занесены на какой-либо материальный носитель, то перед началом процесса кодирования будет выдан запрос о подключении этого носителя. Если же секретный ключ защищен паролем, то, кроме этого, необходимо по запросу программы ввести пароль.
 - 2.5. Для декодирования файлов служит та же программа кодирования, причем в этом случае указывать идентификатор абонента необязательно. В качестве первого обязательного параметра можно указать не имя одного файла, а маску группы файлов.

**ПОРЯДОК СОГЛАСОВАНИЯ РАЗНОГЛАСИЙ
ПО ЭЛЕКТРОННЫМ ДОКУМЕНТАМ, ОФОРМЛЕННЫМ
В СООТВЕТСТВИИ С ТЕХНОЛОГИЕЙ “ЛАН Крипто”**

Стороны на основе взаимного согласия принимают следующий порядок разрешения возможных споров по обязательствам, вытекающим из содержания электронных документов.

1. Стороны принимают в качестве электронных документов специальным образом оформленные блоки информации (файлы, записи баз данных, строки и т.п.), подлинность и авторство которых удостоверяется одновременно цифровыми подписями уполномоченных лиц и декодированием полученного сообщения в осмысленный текст с помощью официально зарегистрированного открытого ключа отправителя.

2. Стороны соглашаются принимать на себя в полном объеме все обязательства, вытекающие из электронных документов, подписанных от их имени цифровыми подписями лиц, открытые ключи которых ("образцы цифровых подписей") зарегистрированы в соответствующем списке (каталоге "образцов цифровых подписей"), если при проверке эти цифровые подписи признаются достоверными и к моменту приема документа не было зафиксировано официального заявления подписавшего лица о дезавуировании своего индивидуального ключа подписывания или программного обеспечения.

Невыполнение любой из сторон этого условия является основанием для расторжения договора по инициативе другой стороны.

3. В случае, если одна из сторон отказывается от принятия на себя обязательств по документу, заверенному ее действующей цифровой подписью и признаваемой подлинной программой проверки другой стороны, то:

- проверяется целостность программного обеспечения сторон путем сравнения используемого программного обеспечения для проверки подписи с эталонным образцом (эталонный образец программного обеспечения для проверки цифровых подписей может по договоренности сторон храниться у одной или каждой из них в запечатанном конверте или храниться по обоюдному согласию сторон у третьей стороны, или предоставляться по запросу фирмой-изготовителем);
- повторно проверяется подлинность электронной подписи с помощью программного обеспечения, соответствующего эталону;

Если подпись признается действительной в результате повторной проверки, а сторона, чьей подписью заверен документ, отказывается принять на себя обязательства по документу, то назначается экспертная комиссия из представителей сторон и/или других, признаваемых сторонами экспертов.

Комиссия на основании изучения спорного документа, ключа для проверки цифровой подписи ответчика на магнитном носителе и распечатки этого ключа, заверенной личной подписью ответчика, проводит дополнительную экспертизу документа и цифровой подписи, а также проверку принадлежности данной

цифровой подписи данному лицу и ее действительность в момент оформления документа.

При выполнении всех перечисленных условий комиссия выносит заключение о подлинности цифровой подписи и ее соответствии содержанию документа, который, тем самым, признается действительным.

4. В случае, если одна из сторон отказывается от приема и рассмотрения документа другой стороны на основании того, что цифровая подпись второй стороны под документом воспринимается программой проверки как фальшивая, либо невозможно декодировать данный документ, то:

- сторона, отказавшая в приеме документа, заверяет по требованию отправителя *) свой официальный отказ от рассмотрения документа своей цифровой подписью и передает его отправителю, а вторая сторона повторно подписывает документ своей цифровой подписью либо повторно кодирует и передает документ;
- если новая цифровая подпись также признается первой стороной недействительной, либо декодирование повторно направленного документа невозможно, то стороны проверяют сохранность своих программ подписания и проверки, а также программ кодирования и генерации ключей путем сравнения их с эталонными образцами.

*) Возможны просьбы повторить передачу подписанного и закодированного документа, которые мотивированы плохим качеством связи, ошибкой оператора и т.д. С точки зрения надежности защиты информации они не являются опасными и могут быть выполнены.

5. Если в результате проверки сохранности программного обеспечения выяснится, что:

- разрушено программное обеспечение у автора документа, -
- отказ другой стороны от рассмотрения документа является правомерным;
- разрушено программное обеспечение у стороны, отказавшейся от приема документа, - она обязана возместить убытки, возникшие у другой стороны вследствие ее отказа от рассмотрения документа, основанием для привлечения к ответственности служит официальный отказ от приема документа;
- не выявлено отличия программного обеспечения ни одной из сторон от эталонного образца - признается несоответствие программного обеспечения техническому описанию используемых алгоритмов, ответственность ложится на фирму-изготовителя программ и алгоритмов.