ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ МЕЖДУ ООО «ВАШ ИНВЕСТИЦИОННЫЙ ПАРТНЕР» И КЛИЕНТАМИ КОМПАНИИ

Инвестиционная компания ООО «Ваш Инвестиционный Партнер» (далее - Компания) разработала настоящий порядок использования электронной цифровой подписи (далее - ЭЦП) при обмене электронными документами между Компанией и ее клиентами, заключившими договора на брокерское обслуживание, путем подписания Соглашения о присоединении……

1. Основные положения

1.1. Правовое регулирование отношений в области использования ЭЦП между Компанией и Клиентами осуществляется в соответствии с Гражданским кодексом РФ, с Федеральными законами от 10.01.2002 N 1-ФЗ "Об электронной цифровой подписи" (далее - Закон об ЭЦП), от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами.
1.2. Действие настоящего документа распространяется на всех клиентов Компании, заключивших договора на брокерское обслуживание, при использовании ими ЭЦП.
1.3. При использования ЭЦП Компания и Клиенты должны руководствоваться действующим законодательством РФ, Положением о порядке организации выдачи и отзыва сертификатов ключей электронных цифровых подписей, а также Регламентом на брокерское и депозитарное обслуживание Компании и другими внутренними документами Компании.
1.5. В настоящем Порядке используются термины и определения, приведенные в приложении 1.

2. Электронная цифровая подпись

2.1. Основы применения электронной цифровой подписи.
2.1.1. В соответствии с технологией ЭЦП при выполнении операции криптозащиты используется пара взаимосвязанных ключей ЭЦП. Один из них - закрытый ключ должен быть известен только его владельцу, а второй - открытый - делается общедоступным.
2.1.2. В процессе информационного обмена уполномоченное лицо подписывает электронный документ своим закрытым ключом и отправляет его получателю. Последний, используя открытый ключ отправителя, проверяет подлинность ЭЦП. Подлинность ЭЦП исключает возможность фальсификации документа (достоверность его гарантируется) и не дает возможности участнику информационного обмена после подписания электронного документа впоследствии отказаться от своего авторства (идентификация авторства).
2.1.3. Компания создает и поддерживает механизм доверенных связей между лицами, использующими ЭЦП.

2.2. Условия использования электронной цифровой подписи.
2.2.1. ЭЦП в электронном документе равнозначна собственноручной
подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:
- сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность ЭЦП в электронном документе;

- ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

2.2.2. Ответственность за неправомерное использование ЭЦП несет уполномоченное лицо - владелец сертификата ключа подписи.

2.2.3. Использование ЭЦП при подписании отчетов Компании и документов необходимо для обеспечения юридической значимости электронного взаимодействия участников договора, перечисленных в пункте 1.3 настоящего Порядка.

2.2.4. При создании ключей ЭЦП для использования при размещении применяется свободно используемое программное обеспечение **VIPSign**.

2.2.5. Порядок получения и использования средств ЭЦП клиентами определен Положением о порядке организации выдачи и отзыва сертификатов ключей электронных цифровых подписей Компании.

2.3 Порядок изготовления ключей ЭЦП

2.3.1. Изготовление сертификатов (в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии) осуществляется клиентами Компании самостоятельно и содержит сведения, необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Данное Заявление подписывается собственноручно владельцем сертификата ключа подписи.

2.3.2. При изготовлении сертификатов ЭЦП клиентами они оформляются в форме документов на бумажных носителях в двух экземплярах сертификата (по форме Приложение №3), которые заверяются собственноручными подписями владельца сертификата и уполномоченного лица Компании, а также печатью Компании. Один экземпляр сертификата выдается владельцу сертификата, второй - остается в Компании.

2.3.3. При издании сертификата в форме бумажного документа в нем фиксируются и заверяются следующие сведения:

- уникальный отпечаток сертификата ключа подписи, даты начала и окончания срока действия сертификата, находящегося в реестре Компании;
- фамилия, имя и отчество владельца сертификата или псевдоним;
- открытый ключ электронной цифровой подписи;
- идентификатор средств ЭЦП, с которыми используется данный открытый ключ ЭЦП;
- сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическую силу (договор №….).

2.3.4. На случай компрометации ключей ЭЦП владельцу сертификата назначается ключевое слово (пароль).

2.3.5. Ключи ЭЦП вводятся в обращение с даты выдачи сертификата ключа подписи. Срок действия закрытого ключа ЭЦП и сертификата – не более 12 месяцев.

2.3.6. После окончания действия сертификата ключа подписи уполномоченное лицо – владелец сертификата прекращает использование соответствующего закрытого ключа ЭЦП, в случае, если не продлевает срок действия.

2.4. Прекращение действия сертификата ключа подписи.

2.4.1. После ввода сертификата в обращение его действие временно или окончательно может быть прервано в связи с наступлением какого-либо события, ведущего к приостановлению действия или аннулированию сертификата.

2.4.2. Действие сертификата может быть приостановлено Компанией на основании заявления клиента или в случае опасения законности применения ЭЦП, или если клиент временно не в состоянии использовать средства ЭЦП.

2.4.3. Действие сертификата по указанию клиента Компании может приостанавливаться на исчисляемый в днях срок.

Компания возобновляет действие сертификата по письменному обращению клиента. В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

2.4.4. Компания также аннулирует сертификат подписи:

- по истечении срока его действия;
- в случае прекращения действия договора брокерского обслуживания, на основании которого оформлен сертификат;
- в случае прекращения сроков действия доверенности уполномоченного лица;
- по заявлению в письменной форме владельца сертификата;
- в иных установленных нормативными правовыми актами или соглашением сторон случаях.

2.4.5. В соответствии с указанием клиента о приостановлении/прекращении действия сертификата ЭЦП или решения Компании, Компания аннулирует сертификат и вносит в реестр сертификатов ключей подписей соответствующую информацию с указанием даты, времени и срока приостановления действия сертификата, а также извещает об этом владельца сертификатата.

2.5. Срок и порядок хранения сертификатов и электронных документов, подписанных ЭЦП.

2.5.1. Срок хранения сертификата ключа подписи в форме электронного документа в Компании составляет не более трех лет. При этом обеспечивается доступ перечисленным в пункте 1.3 настоящего Порядка субъектам для получения информации о подписанных сертификатом ключа документах и копий сертификата.

2.5.2. Срок хранения сертификата в форме электронного документа в Компании после аннулирования сертификата не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи. В соответствии с Законом этот срок составляет три года. По истечении указанного срока хранения сертификат исключается из реестра сертификатов ключей подписей и переводится в
режим архивного хранения. Порядок выдачи копий сертификатов в этот период устанавливается в соответствии с законодательством РФ.

2.5.3. Сертификат в форме документа на бумажном носителе хранится в порядке, установленном законодательством РФ об архивах и архивном деле.

2.5.4. Срок хранения электронных документов, подписанных сертификатом ЭЦП и перечисленных в п.2.5.1 настоящего Порядка, устанавливается в соответствии с требованиями федерального законодательства.

2.6. Подтверждение ЭЦП в электронном документе.

2.6.1. Процедура подтверждения (проверки) ЭЦП в электронном документе включает в себя проверку действительности использованного сертификата на момент проверки или на момент подписания, проверку подлинности ЭЦП и проверку соответствия использования ЭЦП сведениям в сертификате.

2.6.2. При проведении подтверждения ЭЦП в электронном документе пользователь использует средства ЭЦП в соответствии с инструкцией по пользованию этими средствами. Если электронный документ, в котором необходимо проверить электронную цифровую подпись, находится в информационной системе Компании, то следует руководствоваться также инструкцией информационной системы по выполнению этой процедуры. При проведении подтверждения ЭЦП в электронном документе электронная цифровая подпись лица, проводящего подтверждение, не требуется.

2.7. Рассмотрение конфликтных ситуаций, связанных с использованием ЭЦП.

2.7.1. Применение ЭЦП может приводить к конфликтным ситуациям, заключающимся в оспаривании сторонами авторства и/или неизменности содержимого документа, подписанного электронной
цифровой подписью. При этом оспаривающей стороной может выступать: Клиент, или уполномоченное им лицо.

2.7.2. Разбор конфликтных ситуаций, связанных с использованием ЭЦП, проводит комиссия, создаваемая Компанией и Клиентом или уполномоченным им лицом. В состав комиссии должны быть включены представители: оспаривающих сторон, и могут быть включены независимые эксперты, по требования сторон.

2.7.3. Рассмотрение конфликтных ситуаций, связанных с использованием ЭЦП (далее также – конфликтные ситуации), осуществляется с применением специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭЦП содержимому электронного документа.

2.7.4. Разбор конфликтной ситуации проводится для следующих процедур:

- процедура подтверждения ЭЦП с использованием сертификата ключа подписи;
- механизм доказательства обладания закрытым ключом, соответствующим открытому ключу;
- процедура проверки действительности сертификата на бумажном носителе;
- процедура проверки времени отправки/получения электронного документа.

Данный разбор основывается на математических свойствах алгоритма ЭЦП, гарантирующими невозможность подделки значения ЭЦП любым лицом, не обладающим закрытым ключом подписи.

2.8. Процедура подтверждения ЭЦП с использованием сертификата ключа подписи.

2.8.1. Подтверждение ЭЦП в электронном документе осуществляется Компанией по обращению клиента на основании заявления на подтверждение ЭЦП в электронном документе в простой письменной форме.

2.8.2. Обязательным приложением к заявлению на подтверждение ЭЦП в электронном документе является отчуждаемый носитель, содержащий следующие файлы:

- файл, содержащий электронный документ, к которому применена ЭЦП;
- файл, содержащий копию бумажного сертификата действующего ЭЦП клиента подписанный обеими сторонами;
- файл, содержащий список отозванных сертификатов ЭЦП, и

Сертификат, использовавшийся для подписи проверяемого ЭЦП электронного документа клиента, если документ подписан аннулированным сертификатом ЭЦП.

Срок рассмотрения заявления на подтверждение ЭЦП в электронном документе составляет 7 календарных дней с момента его поступления в Компанию.

2.8.3. По результатам рассмотрения заявления на подтверждение ЭЦП в электронном документе заявителю предоставляется ответ в письменной форме, заверенный подписью и печатью Компании.

2.8.4.Ответ должен содержать:

- результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности ЭЦП в электронном документе владельцу;
- детальный отчет по выполненной проверке.

2.8.5.Детальный отчет по выполненной проверке включает сведения:

- время и место проведения проверки;

- основания для проведения проверки;
- сведения об уполномоченных лицах Компании, проводивших проверку (Ф.И.О., образование, специальность, стаж работы, занимаемая должность);
- вопросы, поставленные перед комиссией;
- объекты исследований и материалы по заявлению, представленные для проведения проверки;
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение комиссии, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручными подписями членов комиссии.

2.9. Механизм доказательства обладания закрытым ключом, соответствующим открытому ключу.

2.9.1. Заявления на регистрацию сертификатов ключей подписей, поступающие в Компанию от владельцев ключей подписей, должны содержать собственноручную подпись заявителя. Подтверждение подписи запроса на сертификат из заявления на регистрацию сертификатов и наличие собственноручной подписи заявителя подтверждает, что заявитель является владельцем закрытого ключа, соответствующего открытому ключу из Соглашения о присоединении к Регламенту оказания брокерских услуг на рынке ценных бумаг ООО «Ваш Инвестиционный Партнер».

2.9.2. Процедура проверки действительности сертификата на бумажном носителе, предоставленном клиентом или уполномоченным лицом в Компанию, производится в следующей последовательности:

- заявитель представляет сертификат на бумажном носителе(бумажную копию) с заявлением на проверку действительности, составленным в простой письменной форме;
- уполномоченное лицо Компании производит поиск в Реестре сертификата по параметрам, указанным в предъявленной бумажной копии;
- производится посимвольное визуальное сравнение копий, предъявленных заявителем и найденных в Реестре сертификатов;
- производится оформление заключения (справки) уполномоченным лицом Компании о соответствии или несоответствии находящегося в Реестре сертификата бумажной копии.

В случае отсутствия сертификата в Реестре оформляется заключение от имени уполномоченного лица Компании о невозможности проверки соответствия ввиду отсутствия сертификата в Реестре.

3. Организационные и технические требования к документам, подписываемым с использованием ЭЦП

3.1. Электронные документы, направляемые Компанией своим Клиентам, могут быть созданы с использованием различных программных средств – текстового редактора, электронных таблиц, сгенерированы торговой системой, системами бэк-офиса, депозитария, бухгалтерии и т.д.

3.2. Клиент сохраняет на личный компьютер электронный документ, не подписанный ЭЦП, для контроля в дальнейшем неизменности первоначального документа.

3.3. Подписание электронного документа ЭЦП Клиентом (формирование ЭЦП Клиента) происходит за два этапа:

- Электронный документ, который Клиент должен подписать, загружен Компанией и доступен для в просмотра через web-интерфейс https://webint.vipinvest.ru с использованием действующего SSL-сертификата в разделе «Отчеты».

- Загруженный документ подписывается Клиентом. Созданный файл подписанного ЭЦП Клиента документа автоматически сохраняется на сервер.

3.4. Сервер Компании генерирует электронное письмо с сообщением о факте создания подписанного ЭЦП Коиента документа. Один экземпляр направляется Клиенту, на его зарегистрированный в документах на брокерское обслуживание электронный адрес. Копия письма сохраняется в регистрах учета в локальной сети Компании.

4. Ответственность сторон, использующих ЭЦП

4.1. Компания несет следующие обязательства по отношению к владельцу сертификата ключа подписи:

- обеспечивает работу сертификата ключа подписи обратившимся к нему клиентам, заключившим договор на брокерское обслуживание;
- вносит сертификат ключа подписи в реестр сертификатов ключей подписей;
- ведет реестр сертификатов ключей подписи, обеспечивает его актуальность и возможность свободного доступа к нему владельцев ключей;
- приостанавливает действие сертификата ключа подписи по обращению его владельца;
- уведомляет владельца сертификата ключа подписи о фактах, которые стали известны Компании и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;
- иные установленные нормативными правовыми актами или соглашением сторон обязательствами.
- несет гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

4.2. Владелец сертификата ключа подписи обязан:

- не использовать для ЭЦП открытые и закрытые ключи ЭЦП, если ему известно, что эти ключи используются или использовались ранее;
- хранить в тайне закрытый ключ ЭЦП;
- немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена;
- выполнять порядок и условия использования ЭЦП, изложенные в данном Порядке и Регламенте Компании;
- выполнять условия договора с Компанией;
- своевременно сообщать в Компанию об изменении своих учетных данных, указываемых в подписанных документах;
- выполнять требования технической документации по применению технологии использования ЭЦП.

4.3. Ответственность Клиента. При несоблюдении требований, изложенных в пункте 4.3 настоящего Порядка, возмещение причиненных вследствие этого убытков возлагается на Клиента или уполномоченное лицо, которому клиент делегировал права использования ЭЦП.

5. Порядок внесения изменений и дополнений

5.1. Изменения и дополнения в настоящий Порядок вносятся Компанией и доводятся до сведения Клиентов в установленном порядке.

Приложение № 1
к Порядку использования ЭЦП

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Сайт - часть информационного пространства в сети Интернет, имеющая уникальное имя (адрес в сети Интернет) и физически находящаяся на одном сервере, которую можно посмотреть с любого компьютера, подключенного к сети Интернет с помощью специальной программы.
Сеть Интернет - телекоммуникационная сетьобщего пользования, предназначенная для обмена информацией между компьютерами и другими устройствами в электронной форме.
Сервер - компьютер, подключенный к сети Интернет, предоставляющий клиентам доступ к общим информационным ресурсам системы Интернет-трейдинга и электронным документам и управляющий этими ресурсами.
Компания - Инвестиционная компании ООО «Ваш Инвестционный Партнер»
Электронный документ - документ, в котором информация представлена в электронно-цифровой форме.
Электронный документ, подписанный ЭЦП - электронный документ, снабженный электронной цифровой подписью, позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в первоначальном электронном документе.
Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи~~, а также установить отсутствие искажения информации в электронном документе~~.
Владелец сертификата ключа подписи - физическое лицо - Клиент или уполномоченное им лицо, на имя которого зарегистрирован сертификат ключа подписи и который владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электронные документы).
Средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП;
- подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе;
- создание закрытых и открытых ключей электронных цифровых подписей.

Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах ЭЦП с использованием средств ЭЦП.
Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности ЭЦП в электронном документе.
Сертификат ключа подписи - документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица, которые включают в себя открытый ключ ЭЦП и которые изготавливаются участником информационной системы для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа подписи.
Подтверждение подлинности ЭЦП в электронном документе - положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности ЭЦП в электронном документе владельцу

сертификата ключа подписи и отсутствия искажений в подписанном данной ЭЦП электронном документе.

Компрометация ЭЦП - утрата доверия к тому, что используемое ПО или каналы связи не обеспечивают безопасность информации. К событиям, связанным с компрометацией ЭЦП относятся, включая, но не ограничиваясь, следующие:

- утрата носителей (средств хранения информации с записанными на них электронными документами и ЭЦП);
- утрата носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к служебной информации;
- нарушение правил доступа к носителю информации и паролям;
- возникновение подозрений на утечку информации или ее искажение.

Приложение № 2
к Порядку использования ЭЦП

ТРЕБОВАНИЯ
рабочему месту с использованием ЭЦП

Требования к рабочему месту, оборудованному средствами ЭЦП:
1. Персональный компьютер (ПК) в следующей минимальной конфигурации:
- процессор - не ниже Pentium 4;
- оперативная память - не менее 256 Mb;
- пространство на жестком диске для установки компонентов – не менее 30 Mb:
2. ПК должен быть оснащен следующими программными средствами:
- операционная система Windows 98/Windows 2000/Windows XP/ Windows Vista;
- MS Internet Explorer версии 5.0 и выше;
- свободно распространяемое программное обеспечение VIPSign;
- лицензионное антивирусное программное обеспечение - для защиты от внедрения вредоносных компонентов и гарантии бесперебойной работы компонентов ЭЦП.

Приложение № 3 к Порядку использования электронной цифровой подписи между ООО «Ваш Инвестиционный Партнер» и клиентами, заключившими договора брокерского обслуживания с использованием системы Интернет-трейдинга.

Сертификат
электронной-цифровой подписи

г. Москва «_____» _____ 20___ г.

Инвестиционная компания «Ваш Инвестиционный Партнер» (общество с ограниченной ответственностью), именуемое в дальнейшем «Компания», в лице *Генерального директора Красенков Алексея Юрьевича*, действующего на основании Устава с одной стороны, и _____ именуемый(ое) в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», составили настоящий акт о нижеследующем:

В соответствии с Договором *№ от « » 200 г.*
Клиентом сгенерированы и зарегистрированы в Компании новые криптографические ключи Клиента, уполномоченных подписывать электронными цифровыми подписями, передаваемые в Компанию электронные документы;
Клиент передал, а Компания получила по каналам электронной связи сертификат(ы) ключа электронной цифровой подписи уполномоченных(ого) лиц(а):
Уникальный отпечаток ключа: 72F0 6AEB 8996 7E1A 65C9 E8B7 4ADC 86A3 4595 2BEA
Открытый ключ:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.2 (MingW32)

mQGiBEj1f2oRBADp5RuwsvsJDyZwRZU0huMDMeszKoaeK1bVXarHRB1KPsFP5plD
dd3jdrK1Ja7O1f4n0qzYq/ZhGRbmOAnNCSuf1+i2mR6NmUkol0sCiX9bxVKP5/ND
RGl/ViFOphaMwj417ll06VVJdvFjRqn3tnbWUilMrjCA9h2dOvHqlNN4hwCgj/DN
A4GyvxzdSNJlbMo0yz1zxvMD/j0mtp4V645UarNdqi9LaOTA7AzAuHKsFcP2Jtfj
24s40Q5jhUtWuUo4mykQPfrCi+r419oeIpC1xx1R1gOcWvW9VrKJXIxi8frR9t1O
tpV9BVZnLbTHa2lEPgJFsSrZeoWbE5e5YwAWU3N/mZFr/baCanBq7IyJaMO6Ku3M
OKIQA/42pxHNVo2kFT25YB/g9/ac4fCEY1MIgs5hBUNA+yQQ+3Ko/UMUQeJ6uGPw
OKlejO5Z/+nbpo5xTAUaotygFZhzrXLK2OXbeEjqdbNSN07MtatoAEc0Anv7dltk
VakzLBmz8uMqFS/cz84BPMbXLZDEE30EYx5yJNTujM2Jk4XBV7QtMDAwNSBLdXJ1
c2hpbiAoMTUuMTAuMjAwOCkgPGN1cnVzaGluQG1haWwucnU+iF0EExECAB0FAkj1
f2oGCwkIBwMCBBUCCAMEFgIDAQIeAQIXgAAKCRBK3IajRZUr6vt1AJ4m/gdvFlup
78VFdMIy2iA+NwSUZQCfSRKuHuXFjqrVJbuTYDH4v+WtkieIRgQQEQIABgUCSQBa
BQAKCRBc2+LbXLql4wgeAJ9za7AdNI8un7zd8I5wCHOJfaGJAQCgifPZZMrEbEOq
NH/pz3zfRDSMzd25AQ0ESPV/bRAEAIWZiocQAFCXPNSEfIHTFMjC8hPcN5E7q4Aw
FJjNZyWvLJghELyVShPo4H2nduIBUdNKxE+sJVP9yt1m3VeCl1Y1TzHqdVx8OwNF
jdFP83ZQeaX52IX+IHhS6PAGCoyLTKt77wfPW0Zzayxz7RRS6vYdq3cYD5qDxBqp
JfnAHu0zAAMFA/909v/1hmqJcbEFMr6OcWJnAoro1qIC/M/4SHgHoxcOdXPe6xIl
Gi8JEMUbkJN8toYMAk3JdsXp+ndZZQnZq4nckL28vh0Lgq2KsXuqh4FGhlxZLxLT
QV8vd6tLu77AouxDKiakxZ40dp7oiSSPvaFkMURp1TPWnB9iVuluYlkDo4hGBBgR
AgAGBQJI9X9tAAoJEErchqNFlSvqwE8An1AYms9AdP1J5jCU9TzjRxppTsHNAJ0b
2J7v++eqbo1Envl839NkrQ4ozA==
=JaqJ
-----END PGP PUBLIC KEY BLOCK-----

проверена работа в системе Интернет-трейдинга https://webint.vipinvest.ru/ с рабочего места Клиента в режиме подписи электронных документов.

Активация сертификата ключа электронной цифровой подписи в системе Интернет-трейдинга выполнены Сторонами в полном объеме, система Интернет-трейдинга полностью работоспособна и вводится в эксплуатацию с момента подписания настоящего Сертификата.

Настоящий Сертификат составлен в двух экземплярах, имеющих одинаковую юридическую силу.

КОМПАНИЯ
ООО «Ваш Инвестционный Партнер»

_____/Красенков А.Ю./

М.П.

КИЕНТ
_____

_____

М.П.