УТВЕРЖДЕНЫ
Протоколом Правления
ООО «ТАТАГРОПРОМБАНК»
от «09» АВГУСТА 2016 г. № 36

Председатель Правления

_____/Хайдаров А.Ф./

ПРАВИЛА
АККРЕДИТАЦИИ И ОБСЛУЖИВАНИЯ КЛИЕНТА В СЕРВИСЕ «FAKTURA.RU»

КАЗАНЬ, 2016

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная цифровая подпись (Электронная подпись)	– обязательный реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в электронном документе информации
Электронный документ	– электронное сообщение, распоряжение о переводе денежных средств, заверенное Электронной цифровой подписью, в котором информация представлена в электронно-цифровой форме
Ключ	– общее название пары взаимосвязанных секретного и открытого ключей ***Открытый ключ*** – ключ проверки ЭЦП или открытый ключ шифрования; ***Секретный ключ*** – последовательность символов, известная владельцу Сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств ЭЦП.
Сертификат ключа проверки ЭЦП (Сертификат ключа подписи)	– электронный документ или документ на бумажном носителе, выданный Аккредитованным удостоверяющим центром или доверенным лицом Аккредитованного удостоверяющего центра и подтверждающий принадлежность ключа проверки ЭЦП владельцу Сертификата ключа проверки ЭЦП
Аккредитованный удостоверяющий центр	– Закрытое акционерное общество «Центр Цифровых Сертификатов», ИНН 5407187087, место нахождения: 630055, г. Новосибирск, ул. Шатурская, д. 2
Инструкция по созданию ключа	– порядок действий по генерации ключа и получению сертификата. "Инструкция по созданию ключа на флеш-карте" и "Инструкция по созданию ключа на смарт-карте " размещены в информационно-телекоммуникационной сети «Интернет» по адресам: http://www.tapb.ru и https://cpbank.ru
Средства криптографической защиты информации	– аппаратные и/или программные средства, обеспечивающие применение ЭП и шифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение
Владелец сертификата ключа проверки ЭП (Владелец сертификата ключа подписи)	– физическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки ЭП и которое владеет соответствующим Ключом ЭП, позволяющим с помощью средств ЭП создавать Электронную подпись в Электронных документах (подписывать Электронные документы).
Клиент	– юридическое лицо или индивидуальный предприниматель, заключивший с Банком Соглашение
Сотрудник Клиента	– физическое лицо, на которого Клиентом оформлено Заявление на доступ к системе "ИНТЕРНЕТ-БАНК"
Клиентское рабочее место	– индивидуальный комплекс технических и программных средств Клиента, обеспечивающий подготовку, редактирование, подписание, отправку, поиск, получение и печать ЭД и справочной информации при взаимодействии с Банком.
Ключевой носитель	– флеш-накопитель или иной информационный (материальный) носитель, содержащий ключ либо предназначенный для записи ключа
Защищенный ключевой носитель	– ключевой носитель, технические характеристики которого не позволяют скопировать хранящуюся в нем информацию
Компрометация ключа	– утрата доверия к тому, что используемый секретный ключ недоступен третьим лицам либо утеря ключевой информации вследствие программно-аппаратного сбоя. К событиям, связанным с компрометацией ключа, относятся, включая, но не ограничиваясь, следующие: 1. утрата ключевого носителя; 2. утрата ключевого носителя с последующим обнаружением; 3. увольнение сотрудников, имевших доступ к ключевым носителям; 4. смена руководителя организации 5. утрата ключей от сейфа в момент нахождения в нем ключевого

носителя;
6. временный доступ третьих лиц к ключевому носителю;
7. иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к ключу третьих лиц

Счет – счет Клиента, открытый на основании Договора банковского счета.

Тарифы – Тарифы Банка на расчетно-кассовое обслуживание юридических лиц и предпринимателей без образования юридического лица

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сервис – Сервис "FAKTURA.RU"

Система "ИНТЕРНЕТ-БАНК" – то же что и Сервис

Банк – ООО «ТАТАГРОПРОМБАНК»

УЦ – Аккредитованный удостоверяющий центр

Соглашение – Соглашение об использовании системы «ИНТЕРНЕТ-БАНК»

СКЗИ – Средства криптографической защиты информации

Правила – «Правила аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"» ООО «ТАТАГРОПРОМБАНК»

ЭД – электронный документ

ЭЦП – электронная цифровая подпись

ЭП – то же что и ЭЦП

СЕРТИФИКАТ – сертификат ключа проверки ЭЦП (сертификат ключа подписи)

3. АККРЕДИТАЦИЯ В СЕРВИСЕ.

3.1. Документооборот в Сервисе доступен Клиенту только после выполнения им всех следующих действий:

1. наличие клиентского рабочего места, отвечающего требованиям (Приложение №4),
2. выполнения всех необходимых действий для генерации ключа;
3. получения Банком Заявления на выдачу сертификата и Акта приема-передачи сертификата, подписанных Клиентом.

3.2. Клиент предоставляет в Банк:

- Заявление на доступ к системе «Интернет-Банк» (Приложение № 1) - право подписи может быть предоставлено только сотрудникам указанным в карточке подписей;
- Заявление на подключение уведомлений (Приложение № 2) - при необходимости;
- Заявление на использование доверенных IP-адресов (Приложение № 3) - при необходимости;

3.3. Для использования защищенного ключевого носителя (смарт-карты), Клиент получает в Банке смарт-карту, подписывает акт приема-передачи смарт-карты.

3.4. В соответствии с Инструкцией по созданию ключа, сотрудник Клиента генерирует ключ, получает Сертификат. Инструкция размещена на сайтах http://www.tapb.ru и https://cpbank.ru.

3.5. На основании заявлений уполномоченный сотрудник Банка регистрирует Клиента и/или сотрудников Клиента в Сервисе, выполняет необходимые настройки безопасности.

Если после начала работы в Сервисе Клиенту необходимо подключить новых сотрудников, то Клиент выполняет действия в соответствии с п. 3.2-3.5.

Если после начала работы в Сервисе Клиенту необходимо изменить настройки уведомлений, либо доверенные IP-адреса, Клиент предоставляет в банк "Заявление на подключение уведомлений" (Приложение № 2) либо "Заявление на использование доверенных IP-адресов" (Приложение № 3). При этом новое заявление по указанному в нем сотруднику заменяет собой старое.

4. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ (ОБНОВЛЕНИЕ СЕРТИФИКАТА)

4.1. Срок действия сертификата составляет 1 год с момента генерации сертификата.

4.2. Не позднее, чем за 5 (пять) рабочих дней до даты фактического истечения срока действия сертификата сотрудник Клиента обязан произвести действия, направленные на обновление сертификата в соответствии с инструкцией пользователя для корпоративных клиентов, размещенной на сайте http://www.faktura.ru в разделе "Настройка и поддержка". Поскольку запрос на новый сертификат и акт приема-передачи сертификата формируются в электронном виде, подписываются действующим ключом, представлять в банк документы на бумажном носителе не требуется.

4.3. Если сотрудник Клиента не произвел своевременно плановую смену ключей, его обслуживание в

Сервисе приостанавливается с даты окончания срока действия сертификата (осуществляется автоматическая блокировка просроченных ключей сотрудника Клиента).

4.4. Возобновление обслуживания после автоматической блокировки осуществляется после создания сотрудником Клиента новых ключей в соответствии с п. 3.4-3.5 и представления в Банк Заявления на выдачу сертификата и Акта приема-передачи сертификата, подписанных Клиентом.

5. СМЕНА КЛЮЧЕЙ ВСЛЕДСТВИЕ КОМПРОМЕТАЦИИ

5.1. В случае компрометации ключей Клиент сообщает в Банк о случившемся по телефону или любым другим способом, после чего направляет в Банк 2 (два) экземпляра Уведомления о компрометации ключа (Приложение №6) (далее - «Уведомление»), заверенных печатью и подписью Клиента.

Уведомление принимается к исполнению по рабочим дням.

5.2. При получении от Клиента Уведомления на бумажном носителе, сотрудник Банка указывает на бланке Уведомления дату и время его получения и передает Клиенту второй экземпляр уведомления с отметкой времени регистрации.

5.3. Не позднее 2 (двух) часов после получения Банком Уведомления Банк прекращает прием документов, подписанных ЭЦП, сформированной на скомпрометированном ключе. Если Уведомление получено Банком менее, чем за 2 часа до истечения рабочего дня, то срок исполнения Уведомления может быть перенесен на следующий рабочий день.

5.4. Направление Уведомления означает требование Клиента прекратить прием и исполнение любых ЭД, подписанных ЭЦП, сформированных с использованием скомпрометированного ключа.

5.5. Клиент осуществляет действия для генерации/получения новых ключей и оформления сертификата в соответствии с разделом 3.

6. СОПРОВОЖДЕНИЕ КЛИЕНТОВ

6.1. Клиент обращается в службу поддержки сервиса "FAKTURA.RU" по телефону **8-800-200-92-50:**

– для получения консультаций по работе в Сервисе (в том числе по настройке взаимодействия с бухгалтерскими системами - 1С и т.д.);

– в случае технических ошибок в работе Сервиса, например в функционале:

- Вход в систему
- Отправка платежных документов
- Получение, экспорт выписок
- Доставка SMS уведомлений
- Загрузка платежей, реестров из 1С

6.2. Клиент обращается в Банк к ответственному сотруднику департамента клиентского обслуживания:

– по вопросам прохождения платежей, по поводу запросов направленных в почтовых сообщениях;

– для изменения доступа в Сервисе (подключение новых сотрудников, уведомлений, доверенных IP-адресов);

– для уведомления о компрометации ключа;

6.3. Клиент обращается в Банк к ответственному сотруднику управления пластиковых карт:

– по вопросам зачисления на картсчета по договорам зарплатного проекта

7. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

7.1. Этапы электронного документооборота:

1. формирование ЭД;
2. отправка и доставка ЭД;
3. проверка ЭД;
4. подтверждение получения ЭД Банком;
5. отзыв ЭД;
6. учет ЭД (регистрация входящих и исходящих ЭД);
7. хранение ЭД (ведение архивов ЭД).

7.2. Формирование ЭД осуществляется в следующем порядке:

7.2.1. ЭД оформляется путем заполнения стандартной формы документа, предусмотренной в Сервисе для данного вида ЭД, т.е. внесения данных в форму документа согласно наименованиям полей. При оформлении ЭД Сервис осуществляет автоматический контроль присутствия обязательной информации в

соответствующих полях формы документа. Ключевыми полями ЭД являются все обязательные для данного вида ЭД реквизиты, без наличия которых надлежащее исполнение ЭД является невозможным.

7.2.2. Допускается формирование ЭД «Почтовое сообщение» в виде текстового документа с возможностью вложения в него произвольных файлов.

7.3. Отправка и доставка электронного документа:

7.3.1. ЭД считается исходящим от отправителя, если:

- ЭД подписан с использованием действующего ключа (действующих ключей) отправителя;
- получатель не уведомлен о компрометации действующего ключа (действующих ключей) отправителя;
- ЭД передан получателю средствами Сервиса.

7.3.2. ЭД не считается исходящим от отправителя, если:

- ЭД не прошел проверку на подлинность ЭЦП;
- получатель уведомлен о компрометации ключей отправителя.

7.4. Проверка подлинности доставленного ЭД включает:

- проверку ЭД на соответствие установленному формату для данного вида ЭД;
- проверку подлинности ЭЦП электронного документа;
- проверку соответствия параметров ЭД требованиям Договоров между Банком и Клиентом. В случае положительного результата проверки, ЭД принимается к исполнению или к сведению, в зависимости от типа ЭД.

В случае, если ЭД не проходит контроль правильности оформления или не подтверждается его ЭЦП, Банк не принимает данный ЭД к исполнению/сведению, о чем Клиент автоматически получает извещение в Сервисе. Кроме того, основанием для отказа Банка от исполнения распоряжения Клиента о совершении операции по счету служат:

- недостаток денежных средств на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- наличие ограничений по счету (арест денежных средств, приостановление операций по счету);
- неисполнение или ненадлежащее исполнение требований Банка в части реализации им правил и процедур в сфере противодействия (легализации) доходов, полученных преступным путем и финансированию терроризма;
- отсутствие в Банке документа о продлении полномочий представителей/единоличного исполнительного органа юридического лица;
- наличие неисполненных Клиентом обязательств перед Банком;
- отсутствие Клиента – юридического лица по месту его нахождения;
- неисполнение или ненадлежащее исполнение обязательств, предусмотренных договором банковского счета.

7.5. Подтверждение получения электронного документа:

7.5.1. «Подтверждение» представляет собой ЭД, не имеющий визуального представления, и служит для изменения статуса подтверждаемого ЭД.

7.5.2. Если иное не предусмотрено отдельными договорами между Банком и Клиентом, то ЭД считается неполученным получателем до тех пор, пока отправитель не получил соответствующего электронного документа типа «Подтверждение». В случае платежных документов (в частности, ЭД "Платежное поручение"), получение ЭД отображается в Сервисе состоянием электронного документа "Принят банком".

7.5.3. Если подтверждение не получено отправителем в течение одного часа рабочего времени Банка с момента отправки, то отправитель может уведомить получателя о неполучении подтверждения.

7.5.4. В случае подозрения на несанкционированный доступ к счету, на фальсификацию электронного сообщения, сотрудник Банка дополнительно получает телефонное подтверждение от Клиента на исполнение документа.

7.6. Отзыв электронного документа.

7.6.1. Клиент вправе отозвать ЭД в день отправки путем направления получателю электронного документа «Заявление на отзыв документа», если оно предусмотрено для данной категории ЭД.

7.6.2. В Заявлении на отзыв документа должна указываться причина отзыва ЭД.

7.6.3. ЭД может быть отозван только до начала его исполнения получателем. Банк вправе отказать в отзыве отправителю в случае невозможности отзыва ЭД.

7.7. Учет ЭД.

7.7.1. Учет ЭД, отправленных через Сервис, осуществляется оператором Сервиса ЗАО «Биллинговый центр» (ИНН 5401152049, местонахождение: 630128, г. Новосибирск, ул. Инженерная, д. 4а)

7.8. Хранение ЭД.

7.8.1. Архивное хранение ЭД осуществляется в соответствии с действующим законодательством РФ, а также Правилами работы сервиса «FAKTURA.RU».

7.9. Аутентификация клиента.

7.9.1. Для аутентификации клиента при подтверждении клиентом права доступа в систему "ИНТЕРНЕТ-БАНК" используется пароль многоразового действия. Возможность использования одноразового кода подтверждения при входе в систему "ИНТЕРНЕТ-БАНК" подключается на основании Заявления на подключение уведомлений (Приложение №2).

7.9.2. Пароль многоразового действия и одноразовый код подтверждения для аутентификации клиента при осуществлении переводов денежных средств в системе "ИНТЕРНЕТ-БАНК" не используются.

7.10. Параметры операций.

7.10.1. Перечень устройств, с использованием которых может осуществляться доступ к системе "ИНТЕРНЕТ-БАНК", может быть ограничен на основании Заявления на использование доверенных IP-адресов (Приложение № 3). Ограничения по иным параметрам операций (в том числе: максимальная сумма перевода денежных средств за одну операцию и (или) за определенный период времени; перечень возможных получателей денежных средств; перечень услуг; временной период, в который могут быть совершены переводы денежных средств) не используются.

Приложение № 1
к Правилам аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"
В ООО «ТАТАГРОПРОМБАНК»

ЗАЯВЛЕНИЕ
на доступ к системе "ИНТЕРНЕТ-БАНК"

ДАТА

В соответствии с условиями соглашения к договору №_____от _____:

1. Прошу предоставить доступ к системе "ИНТЕРНЕТ-БАНК", подключить Сертификат

ДЛЯ КЛИЕНТА (ЗАПОЛНЯЕТСЯ ПЕЧАТНЫМИ БУКВАМИ)

НАИМЕНОВАНИЕ КЛИЕНТА	
ИНН/КПП	
ЮРИДИЧЕСКИЙ АДРЕС	

БАНКОВСКИЕ СЧЕТА (НЕ УКАЗЫВАЮТСЯ В СЛУЧАЕ ПОДКЛЮЧЕНИЯ ТОЛЬКО ДЛЯ ПЕРЕДАЧИ ПОЧТОВЫХ СООБЩЕНИЙ)

НОМЕР СЧЕТА	
НОМЕР СЧЕТА	
НОМЕР СЧЕТА	

СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ СЕРТИФИКАТА (ЗАПОЛНЯЕТСЯ ПЕЧАТНЫМИ БУКВАМИ)

ДОЛЖНОСТЬ			
ФАМИЛИЯ			
ИМЯ			
ОТЧЕСТВО			
ДОКУМЕНТ, УДОСТОВЕРЯЮЩИЙ ЛИЧНОСТЬ (ВИД, СЕРИЯ, НОМЕР, КЕМ И КОГДА ВЫДАН)			
АДРЕС РЕГИСТРАЦИИ		ДАТА РОЖДЕНИЯ	
E-MAIL		ТЕЛЕФОН	
С обработкой персональных данных в соответствии с требованиями Федерального Закона № 152-ФЗ от 27.07.2006 г. "О персональных данных" согласен(на) _____ (подпись владельца сертификата)			

ТИП ПОДПИСИ ПОД ДОКУМЕНТОМ

ВЫБРАТЬ ОДИН ВАРИАНТ	☐ ЕДИНСТВЕННАЯ (ПЕРВАЯ)	☐ ВТОРАЯ	☐ ПОДТВЕРЖДАЮЩАЯ	☐ НЕ ИМЕЕТ ПРАВА, НО МОЖЕТ:	☐ создавать документы ☐ просматривать выписки

2. Настоящим Клиент заявляет, что любые действия, которые будут совершены Владельцем Сертификата, на основании полученного в связи с настоящим Заявлением ключами являются действиями, совершаемыми от имени Клиента, по его указанию и связаны с участием Клиента в электронном документообороте.

КЛИЕНТ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА
руководитель			
главный бухгалтер			

М.П.

ОТМЕТКА БАНКА
ПОДПИСЬ КЛИЕНТА ПРОВЕРЕНА ПО КАРТОЧКЕ ОБРАЗЦОВ ПОДПИСЕЙ И СООТВЕТСТВУЕТ ОРИГИНАЛУ.

ДОЛЖНОСТЬ СОТРУДНИКА БАНКА	ПОДПИСЬ	ДАТА

МЕСТО ШТАМПА

Приложение № 2
к Правилам аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"

В ООО «ТАТАГРОПРОМБАНК»

ЗАЯВЛЕНИЕ
на подключение уведомлений

ДАТА

От Клиента _____

_____
(указать ИНН, полное наименование юридического лица/ полное ФИО индивидуального предпринимателя)

1	В РАМКАХ СОГЛАШЕНИЯ ОБ ИСПОЛЬЗОВАНИИ СИСТЕМЫ «ИНТЕРНЕТ-БАНК» ПРОШУ (отметить нужное) ☐ - осуществлять уведомления ☐ - отключить уведомления ПО СЛЕДУЮЩЕМУ(ИМ) ТЕЛЕФОНУ(АМ) / ЭЛЕКТРОННОМУ(ЫМ) АДРЕСУ(АМ) СОТРУДНИКА(ОВ): **Внимание!** **Указываются только сотрудники организации, зарегистрированные в сервисе**

ФИО Сотрудника организации	

Отметить нужное (обязательно к заполнению одно из полей):

☐ Установка дополнительного пароля на вход в систему (При входе в систему идентифицируется не только ключ электронной подписи, но и дополнительно разовый пароль, высланный на мобильный телефон)

☐ Уведомление при входе в систему

☐ Уведомление об отправке платежей в Банк

Мобильный телефон Основной	+7										
Мобильный телефон Дополнительный	+7										
E-mail											

С обработкой персональных данных в соответствии с требованиями
Федерального Закона № 152-ФЗ от 27.07.2006 г. "О персональных данных" согласен(на) _____ (подпись сотрудника)

2	**ОТПРАВКУ УВЕДОМЛЕНИЙ НА ДОПОЛНИТЕЛЬНЫЙ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА КЛИЕНТ АКТИВИРУЕТ В СЕРВИСЕ САМОСТОЯТЕЛЬНО**
3	ОТВЕТСТВЕННОСТЬ ЗА ПРАВИЛЬНОСТЬ УКАЗАНИЯ ТЕЛЕФОННЫХ НОМЕРОВ И ЭЛЕКРОННЫХ АДРЕСОВ НЕСЕТ КЛИЕНТ
4	ДАННОЕ ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ УВЕДОМЛЕНИЙ ЯВЛЯЕТСЯ ОСНОВАНИЕМ ДЛЯ ОТКЛЮЧЕНИЯ ВСЕХ РАНЕЕ ПРИНЯТЫХ БАНКОМ ЗАЯВЛЕНИЙ КЛИЕНТА НА ПОДКЛЮЧЕНИЕ УВЕДОМЛЕНИЙ
5	РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ

Разрешаю Банку в одностороннем порядке принимать дополнительные меры обеспечения безопасности и надлежащего обслуживания в системе «Интернет-Банк». С Тарифами за предоставление услуги ознакомлен и согласен.

ФИО:_____	Подпись	Печать

ОТМЕТКА БАНКА
ПОДПИСЬ КЛИЕНТА ПРОВЕРЕНА ПО КАРТОЧКЕ ОБРАЗЦОВ ПОДПИСЕЙ И СООТВЕТСТВУЕТ ОРИГИНАЛУ, ОБЯЗАТЕЛЬНЫЕ ДЛЯ ЗАПОЛНЕНИЯ ПОЛЯ ОТМЕЧЕНЫ

ДОЛЖНОСТЬ СОТРУДНИКА БАНКА	ПОДПИСЬ	ДАТА

МЕСТО ШТАМПА

Приложение № 3
к Правилам аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"

В ООО «ТАТАГРОПРОМБАНК»

ЗАЯВЛЕНИЕ
на использование доверенных IP-адресов

ДАТА

От _____

_____
(указать ИНН, полное наименование юридического лица/ полное ФИО индивидуального предпринимателя)

1	**В РАМКАХ СОГЛАШЕНИЯ ОБ ИСПОЛЬЗОВАНИИ СИСТЕМЫ «ИНТЕРНЕТ-БАНК» ПРОШУ ИСПОЛЬЗОВАТЬ ДОВЕРЕННЫЕ IP-АДРЕСА СОТРУДНИКА(ОВ):** **Внимание!** **Указываются только сотрудники организации, зарегистрированные в сервисе**

1) ФИО Сотрудника организации	

Отметить что-то одно:
☐ Разрешить вход с ЛЮБЫХ IP-адресов. Риск последствий принятия к исполнению распоряжений с иных IP-адресов, а также риск передачи Электронных документов неуполномоченными лицами понимаю и принимаю на себя.
☐ Разрешить вход только с доверенных IP-адресов:

IP-адреса или диапазоны	

С обработкой персональных данных в соответствии с требованиями
Федерального Закона № 152-ФЗ от 27.07.2006 г. "О персональных данных" согласен(на) _____ (подпись сотрудника)

2) ФИО Сотрудника организации	

Отметить что-то одно:
☐ Разрешить вход с ЛЮБЫХ IP-адресов. Риск последствий принятия к исполнению распоряжений с иных IP-адресов, а также риск передачи Электронных документов неуполномоченными лицами понимаю и принимаю на себя.
☐ Разрешить вход только с доверенных IP-адресов:

IP-адреса или диапазоны	

С обработкой персональных данных в соответствии с требованиями
Федерального Закона № 152-ФЗ от 27.07.2006 г. "О персональных данных" согласен(на) _____ (подпись сотрудника)

3		**РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ**		
ФИО:_____			Подпись	Печать

ОТМЕТКА БАНКА
ПОДПИСЬ КЛИЕНТА ПРОВЕРЕНА ПО КАРТОЧКЕ ОБРАЗЦОВ ПОДПИСЕЙ И СООТВЕТСТВУЕТ ОРИГИНАЛУ.

ДОЛЖНОСТЬ СОТРУДНИКА БАНКА	ПОДПИСЬ	ДАТА

МЕСТО ШТАМПА

Приложение № 4
к Правилам аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"

Требования к рабочему месту КЛИЕНТА

Операционные системы: Windows 2000/XP/Vista/7/8
Браузер: IE 7.0 и выше (обязательно с поддержкой 128-битного шифрования).
Прокси-сервер должен обеспечивать возможность устанавливать исходящие соединения по 443 порту (SSL), а также возможность загружать файлы размером более 1МБ.

Настройки англоязычной версии Internet Explorer:

- Закладка General: Settings/Check for newer version of stored pages – Automatically
- Закладка Advanced: Do not save encrypted pages to disk -Checked Use HTTP 1.1 through proxy connection - Checked Use SSL 2.0 - Checked Use SSL 3.0 - Checked
- Закладка Security Download signed ActiveX controls - Prompt Run ActiveX Controls and plugins -Enable Script ActiveX controls marked safe for scripting - Enable Allow META REFRESH - Enable

Настройки русскоязычной версии Internet Explorer:

- Закладка Общие Параметры – Проверять наличие обновления сохраненных страниц - Автоматически
- Закладка Дополнительно SSL 2.0 – Checked SSL 3.0 – Checked Использовать HTTP 1.1 через прокси-соединения - Checked Не сохранять зашифрованные страницы на диск - Checked
- Закладка Безопасность Выполнять сценарии элементов ActiveX, помеченных как безопасные – Разрешить Загружать подписанные элементы ActiveX - Предлагать Запуск элементов ActiveX и модулей подключения – Разрешить Разрешить метаобновление - Разрешить

Дополнительные настройки браузера Internet Explorer 10/11:

1. Откройте сайт www.faktura.ru в браузере Internet Explorer.
2. Нажмите кнопку «Alt», выберите меню «Сервис», затем «Параметры просмотра в режиме совместимости».
3. Добавьте «faktura.ru», «authority.ru» в список.

Приложение № 5
к Правилам аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"

УСЛОВИЯ
использования электронного средства платежа

Для безопасного использования сервиса "FAKTURA.RU" как электронного средства платежа, Клиент должен следовать следующим рекомендациям:

1. Общие меры безопасности:

- обеспечить постоянную доступность номера мобильного телефона/адреса электронной почты, на которые подключены уведомления, и ежедневно проверять SMS-сообщения/сообщения электронной почты;
- в случае утраты мобильного телефона, незамедлительно заблокировать SIM-карту;
- при получении сообщения в формате SMS либо в электронном формате по электронной почте либо звонка по телефону, Клиент обязан убедиться, что такое сообщение/звонок исходит именно от Банка или уполномоченного им лица;
- при получении сообщений, следует отказаться от выполнения действий, изложенных в сообщениях в следующих случаях:
  - сообщение поступило не от Банка или уполномоченного им лица;
  - сообщение поступило не с официальных телефонных номеров Банка, которые указаны на официальном сайте Банка в сети Интернет;
  - запрашиваемые в сообщении действия требуют срочного ответа Клиента;
  - сообщение требует предоставить, обновить или подтвердить персональную информацию Клиента (например ПИН-код, номер телефона, имя пользователя, пароль, иную ключевую/парольную информацию);
  - сообщение содержит форму для ввода персональной информации Клиента;
  - в сообщении содержится информация, что на счёт Клиента непредвиденно для него поступили денежные средства;
  - в сообщении содержится просьба войти в систему ДБО по указанной ссылке;
  - полученная информация вызывает любые сомнения или подозрение на мошенничество
- ежедневно в Сервисе проверять состояние всех своих счетов, включая остаток по счету, доступный баланс по счету, операции по счету и незамедлительно уведомлять Банк лично о наличии ошибок, неточностей или возникновении вопросов в отношении информации, содержащейся в Сервисе.
- соблюдать рекомендации по обеспечению безопасности, размещенные на сайте Банка, на сайте Faktura.ru

2. Рекомендации по обеспечению безопасности при работе в Интернет:

- использовать только лицензионное системное и прикладное программное обеспечение, а так же обеспечить их регулярное обновление;
- применять средства антивирусной защиты и специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение, обеспечивая при этом своевременное обновление антивирусных баз, а также осуществлять еженедельную антивирусную проверку, а так же проверку после любых действий сторонних лиц, в том числе и технических специалистов;
- исключить возможность посещения интернет-сайтов сомнительного содержания с компьютера, на котором ведется работа в Системе;
- обеспечить защиту от несанкционированного доступа к компьютеру, на котором установлено программное обеспечение Системы, а так же запретить или существенно ограничивать использование любых средств удалённого доступа;
- установить сложные пароли для всех учётных записей, имеющих право входа на компьютер, на котором ведется работа в Системе, а также осуществлять их периодическую смену;
- не использовать Сервис если соединение с сайтом системы ДБО не зашифровано (отсутствует индикация работы браузера в защищенном режиме) или при его посещении возникают ошибки проверки подлинности сертификата;
- не вводите свои средства авторизации на сайтах, адреса которых отличны от https://faktura.ru, https://www.authority.ru;
- самостоятельно указывайте адрес сайта в соответствующем поле браузера;

- избегайте работы с системой «Интернет-Банк» в публичной среде, такой, как интернет кафе, социальные точки доступа в интернет, компьютеры друзей и тому подобное, а также в присутствии посторонних лиц;
- подключите SMS-уведомление о входе в систему;
- при входе в Сервис необходимо проверять дату и время последнего входа. В случае подозрения на несанкционированный доступ к системе либо компрометацию ключевой/парольной информации, незамедлительно сообщить об этом в Банк своему куратору, а затем лично в письменной форме;
- завершать работу в Сервисе в соответствии с установленными процедурами. Не закрывайте окно браузера, без предварительного выхода из Сервиса. Если Клиент не выполнял вход в Сервис, но при этом получил сообщение о входе, незамедлительно сообщить об этом в Банк своему куратору, а затем лично в письменной форме.

3. **Рекомендации по обеспечению безопасности при использовании Сервиса на мобильных устройствах:**
   - использовать на мобильных устройствах только официальные приложения, предоставленные оператором Сервиса.
   - не использовать несанкционированные модификации программного обеспечения мобильных устройств (взлом прошивки, rooting, jailbreaking);
   - не использовать мобильные устройства для доступа к полнофункциональной версии Сервиса;
4. **Рекомендации по обеспечению безопасности ключевой информации:**
   - необходимо хранить ключи ЭЦП только на внешних носителях (дискеты, флеш-накопители и др.), а не на жёстких или сетевых дисках компьютера. Не записывать на данный носитель какую либо другую информацию;
   - **при возможности, использовать защищенный ключевой носитель (смарт-карту)**. Секретный ключ ЭЦП технически невозможно считать из смарт-карты и сделать копию, отправить по электронной почте или сохранить на другом носителе;
   - ключевой носитель необходимо извлекать из компьютера каждый раз после завершения использования, а так же не отлучатся от рабочего места во время работы в Системе;
   - обязательно сменить выданные пароли для смарт-карты (PIN и PUC коды);
   - не допускать использования простых паролей (123456, qwerty, дата рождения, номер телефона и т.п.), а также осуществлять периодическую их смену. Ни в коем случае не записывать пароли на бумажных листках (или в текстовых файлах на компьютере), не оставлять их в легкодоступных местах;
   - никому, включая работников Банка, ни при каких условиях не сообщайте пароль на ключ;
   - используйте виртуальную клавиатуру при наборе пароля;
   - не допускать передачу ключевого носителя кому-либо, в том числе техническим специалистам для проверки работы Системы, настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец ключа ЭЦП обязан лично подключать ключевой носитель к компьютеру и вводить в Систему пароль.

Приложение № 6
к Правилам аккредитации и обслуживания клиента в сервисе "FAKTURA.RU"

В ООО «ТАТАГРОПРОМБАНК»

УВЕДОМЛЕНИЕ
о компрометации ключа

ДАТА

Настоящим уведомляю о компрометации ключа

ВЛАДЕЛЕЦ СЕРТИФИКАТА (ФИО)	
НАИМЕНОВАНИЕ КЛИЕНТА	
ИНН/КПП	
ПРИЧИНА КОМПРОМЕТАЦИИ	☐ ПРЕКРАЩЕНИЕ ПОЛНОМОЧИЙ ВЛАДЕЛЬЦА СЕРТИФИКАТА ☐ СБОИ ПРОГРАММНО-АППАРАТНОГО ОБЕСПЕЧЕНИЯ ☐ УТЕРЯ ☐ ДРУГОЕ _____

КЛИЕНТ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ

М.П.

ОТМЕТКА БАНКА

Отметка о получении Уведомления Банком

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА	ВРЕМЯ

М.П.