

ДОГОВОР № \_\_\_\_\_  
на предоставление услуг электронной коммерции  
по картам международных платежных систем через Интернет

г. \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 201\_ г.

Национальный банк ВЭД РУ, именуемый в дальнейшем «БАНК», в лице \_\_\_\_\_ при \_\_\_\_\_, действующего на основании доверенности \_\_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ г., и \_\_\_\_\_, именуемое в дальнейшем «ТСП», в лице \_\_\_\_\_ (ФИО, должность), действующего на основании Устава, далее совместно именуемые «Стороны», заключили настоящий Договор (далее – ДОГОВОР) о нижеследующем:

### 1. ТЕРМИНОЛОГИЯ

АВТОРИЗАЦИЯ	процедура запроса и последующего получения ТСП от ПРОВАЙДЕРА УСЛУГ разрешения на проведение операции с использованием КАРТЫ на Интернет - площадке. Подтверждение содержит уникальный код, идентифицирующий каждую конкретную операцию. Наличие кода в ответе, полученном ТСП от ПРОВАЙДЕРА услуг, является разрешением проведения операции с использованием КАРТЫ.
АПК	Специализированный автоматизированный программный комплекс по обработке операций МПС, в т.ч. по оплате товаров (работ, услуг) через Интернет, установленный у ПРОВАЙДЕРА УСЛУГ.
ИНТЕРНЕТ-ПЛОЩАДКА	Интернет-ресурс ТСП или его партнеров, включающий в себя САЙТ в сети Интернет, позволяющий ТСП принимать и обслуживать заказы на приобретение товаров (проведение работ, оказание услуг) через Интернет.
КАРТА	Банковская платежная карта, эмитированная ЭМИТЕНТОМ клиенту – его держателю под эгидой МПС, указанной в Приложении 1 к ДОГОВОРУ.
ТРАНЗАКЦИЯ	Безналичная операция в иностранной валюте, совершаемая ДЕРЖАТЕЛЕМ при помощи Карты, с обязательным проведением АВТОРИЗАЦИИ.
КОМИССИЯ	Вознаграждение, причитающееся БАНКОМ за предоставленные ТСП УСЛУГИ по ДОГОВОРУ.
ПРОВАЙДЕР УСЛУГ	БАНК или компания, заключившая с БАНКОМ договор на оказание УСЛУГ в соответствии со СТАНДАРТАМИ.
МПС	Ведущая международная платежная система, с которой БАНК имеет соглашение на предоставление УСЛУГ.
САЙТ	Совокупность информации, способа ее представления и технических средств, объединенная, как правило, одной темой и/или целью, которая дает возможность пользователю, подключенному к Интернет и имеющему соответствующие технические средства, получить доступ к этой информации.
СТАНДАРТЫ	Международные стандарты, в т.ч. утвержденные МПС в части обеспечения безопасности (3D Secure, Verified by Visa, MasterCard SecureCode, UCAF, SecurePay, BC Card/Smartro).
ТАРИФ	Тарифы комиссионного вознаграждения за выполнение поручений клиентов – физических и юридических лиц БАНКА
ПРАВИЛА УСЛУГИ	Руководство по предоставлению УСЛУГ ТСП. Услуги электронной коммерции по картам МПС, в соответствии со СТАНДАРТАМИ.
ЭКВАЙЕР	Финансовый институт, являющийся участником МПС и

	обеспечивающий расчеты с ТСП по операциям, совершенным с использованием КАРТ.
ЭМИТЕНТ	Финансовый институт, являющийся участником МПС и осуществляющий эмиссию КАРТ.
PCI DSS	Стандарт безопасности платежных систем.

## 2. ПРЕДМЕТ ДОГОВОРА

Предметом настоящего ДОГОВОРА является определение взаимоотношений Сторон в связи с реализацией ТСП товаров (работ, услуг) на САЙТЕ/ИНТЕРНЕТ-ПЛОЩАДКЕ с приемом оплаты с использованием КАРТЫ и организацией БАНКОМ проведения таких ТРАНЗАКЦИЙ с применением АПК для перечисления на счета ТСП денежных средств.

## 3. ПРАВА И ОБЯЗАННОСТИ БАНКА

### 3.1. БАНК обязуется:

**3.1.1.** Обеспечить ТСП предоставление доступа к АПК для проведения операций по оплате товаров (работ, услуг) на САЙТЕ/ИНТЕРНЕТ-ПЛОЩАДКЕ с использованием КАРТ.

**3.1.2.** Организовать с применением АПК, указанного в п. 3.1.1 ДОГОВОРА, проведение ТРАНЗАКЦИЙ, осуществляемых с использованием КАРТ на САЙТЕ/ИНТЕРНЕТ-ПЛОЩАДКЕ, в режиме 24/7.

**3.1.3.** Организовать прием от ТСП и обработку авторизованных ТРАНЗАКЦИЙ, проведенных законными держателями КАРТ.

**3.1.4.** Осуществлять перечисление денежных средств, оплаченных посредством КАРТ, на расчетный счет ТСП, указанный в Разделе 10 ДОГОВОРА, в течение 3 банковских дней с даты обработки БАНКОМ выставленных МПС авторизованных ТРАНЗАКЦИЙ, за исключением случаев по пунктам 3.2.7 – 3.2.8 и 3.2.9.

**3.1.5.** Хранить банковскую и коммерческую тайны ТСП и держателей КАРТ, ставшие известными БАНКУ в результате выполнения условий ДОГОВОРА.

**3.1.6.** Обеспечить безопасность проведения операций по оплате товаров/услуг картой на САЙТЕ/ИНТЕРНЕТ-ПЛОЩАДКЕ.

**3.1.7.** Ежемесячно не позднее 5-го числа месяца, следующего за расчетным, предоставлять ТСП счет-фактуру и акт об оказанных УСЛУГАХ.

### 3.2. БАНК вправе:

**3.2.1.** Получать у ТСП необходимую для выполнения обязательств по настоящему ДОГОВОРУ информацию.

**3.2.2.** Без дополнительных распоряжений (без акцепта) ТСП списывать со счета ТСП в БАНКЕ, выставлять платежные требования (без акцепта) в другие БАНКИ, денежные средства по уплате КОМИССИИ в размере, предусмотренном ТАРИФОМ БАНКА, а также иных комиссии и выставлении (таких как chargeback и representment) которые были получены от платежных систем по данному ТСП.

**3.2.3.** В одностороннем порядке прекратить проведение АВТОРИЗАЦИИ ТРАНЗАКЦИЙ при нарушении ТСП, ПРАВИЛ по Приложению 2 к ДОГОВОРУ.

**3.2.4.** направить ТСП в течение 1 (одного) рабочего дня соответствующее письменное уведомление о прекращении АВТОРИЗАЦИИ ТРАНЗАКЦИЙ.

**3.2.5.** Проводить совместный/односторонний плановый/внеплановый аудит ТСП на предмет выявления мошеннических операций с КАРТАМИ, предоставления ТСП покупателям несогласованных с БАНКОМ товаров (работ, услуг) и подставных САЙТОВ/ИНТЕРНЕТ-ПЛОЩАДОК.

**3.2.6.** Незамедлительно заблокировать все АВТОРИЗАЦИИ, если установлены факты, что реализуемые товары (работы, услуги) на САЙТЕ/ИНТЕРНЕТ-ПЛОЩАДКЕ не соответствуют заявленной деятельности, и/или присутствуют в списке запрещенных товаров согласно Приложению 4 настоящего ДОГОВОРА и/или САЙТ/ИНТЕРНЕТ-ПЛОЩАДКА занимается обналичиванием средств.

**3.2.7.** Банк вправе не возмещать ТСП денежные средства при возникновении спорных ситуаций, если банк получил Fraud Report (отчет о мошенничестве) или Chargeback (отказ от транзакции) / representment (повторный отказ от транзакции) по проведенным транзакциям до выяснения всех обстоятельств, которые по правилам платежных систем могут составлять от одного до четырех месяцев.

**3.2.8.** Банк вправе приостановить зачисление (замораживание) денежных средств на счет ТСП до полной проверки подозрительных транзакций, которые попали в программу мониторинга Fraud Guard или Visa Fraud Monitoring Program, направив запрос в банки - эмитенты.

**3.2.9.** Банк вправе вернуть денежные средства банкам эмитентам при выявлении международной платежной системой (Visa, MasterCard или UPI) в транзакциях ТСП подозрительную активность и заведении дела по защите брэнда, или при превышении порогового лимита по программе мониторинга подозрительных транзакций платежных систем.

**3.2.10.** Банк оставляет за собой право проводить авторизации с карт, у которых не поддерживается 3D Secure авторизации

## **4. ПРАВА И ОБЯЗАННОСТИ ТСП**

### **4.1. ТСП обязуется:**

**4.1.1.** Исполнять ПРАВИЛА ДОГОВОРА, указанные в Приложении 2 к нему.

**4.1.2.** Обеспечить соответствие ИНТЕРНЕТ-ПЛОЩАДКИ или САЙТА стандарту безопасности МПС PCI DSS.

**4.1.3.** Принимать оплату товаров (работ, услуг) посредством КАРТ по ценам, не превышающим цены на эти товары (работы, услуги) при их оплате в наличной форме.

**4.1.4.** в случае отказа клиента от товара (работ, услуг), обеспечить возврат средств в соответствии с ПРАВИЛАМИ, при этом возврат средств может быть выполнен в виде:

- ТРАНЗАКЦИИ отмены – электронно через персональную страницу ТСП на специальном сайте БАНКА до передачи инкассированного пакета ТРАНЗАКЦИИ;
- ТРАНЗАКЦИИ возврата – электронно или в виде «Формы заявки о возврате средств» согласно Приложению 3 к настоящему ДОГОВОРУ, в том числе при невозможности оформления ТРАНЗАКЦИИ отмены.

**4.1.5.** Оплачивать УСЛУГИ БАНКА по ДОГОВОРУ в порядке, предусмотренном Разделом 5 ДОГОВОРА.

**4.1.6.** Разместить на САЙТЕ информацию, касающуюся обеспечения конфиденциальности данных покупателей и обеспечения безопасности платежей в соответствии с разделами 4, 5 Приложения 2 к ДОГОВОРУ, а также разделами, регламентирующими вопросы безопасности и порядок борьбы с мошенничеством на САЙТЕ ПРОВАЙДЕРА УСЛУГ.

**4.1.7.** Осуществлять хранение информации по операциям с использованием КАРТ (реестры, расписки покупателей в получении товаров (работ, услуг), поручения на дебетование КАРТЫ и пр.) и отчетов по операциям не менее 18 месяцев с даты совершения ТРАНЗАКЦИИ, и передавать их БАНКУ по первому требованию.

**4.1.8.** Согласовывать с БАНКОМ дизайн платежной страницы ИНТЕРНЕТ-ПЛОЩАДКИ(ОК), включая электронные варианты рекламных наклеек с логотипом МПС, указанных в Приложении 1 к ДОГОВОРУ.

**4.1.9.** В обязательном порядке предоставить в БАНК следующую информацию:

- о перечне товаров (работ, услуг), предоставляемых ИНТЕРНЕТ- ПЛОЩАДКОЙ(АМИ) покупателям с указанием мин/сред/макс цены, квитанции почтовых служб об отправке товара;
- о доменном имени САЙТА ИНТЕРНЕТ-ПЛОЩАДКИ(ОК) и о любых его изменениях.
- информацию о IP-адресах, с которых осуществлена транзакция САЙТА ИНТЕРНЕТ-ПЛОЩАДКИ(ОК) и о любых их изменениях.

**4.1.10.** Не реализовывать товары, запрещенные к продаже согласно законодательству Республики Узбекистан. Перечень запрещенных товаров приведен в Приложении 4 к настоящему ДОГОВОРУ.

**4.1.11.** Предоставить БАНКУ постоянный доступ к электронным журналам и/или базам данных регистрации операций каждого САЙТА/ИНТЕРНЕТ-ПЛОЩАДКИ.

**4.1.12.** В срок, установленный БАНКОМ, предоставлять БАНКУ отчет по операциям, которые вызвали подозрение в совершении мошенничества с КАРТАМИ и/или в предоставлении ТСП несогласованных с БАНКОМ товаров (работ, услуг).

**4.1.13.** На регулярной основе осуществлять проверку ИНТЕРНЕТ-ПЛОЩАДКИ и веб-сайт на наличие, вирусов и уязвимостей, вредоносных, рекламных программ и троянов, из-за которых может иметь место компрометация (доступ посторонних лиц к данным клиентов и их КАРТ в результате незаконных действий).

**4.1.14.** Незамедлительно в письменном виде информировать БАНК обо всех изменениях, связанных с платежными реквизитами, характером предоставляемых работ, услуг и реализуемых товаров, об изменениях иных документов и другой информации о ТСП, предоставленных БАНКУ ранее.

**4.1.15.** Хранить банковскую и коммерческую тайны БАНКА и держателей КАРТ, ставшие известными ТСП в результате выполнения условий ДОГОВОРА.

#### **4.2. ТСП вправе:**

**4.2.1.** Требовать от БАНКА своевременного возмещения сумм (за исключением случаев по пунктам 3.2.7 – 3.2.8 и 3.2.9) операций по оплате товаров (работ, услуг), совершенных с использованием КАРТ на ИНТЕРНЕТ-ПЛОЩАДКЕ.

**4.2.2.** Ссылаться на возможность обслуживания КАРТ в собственных рекламных материалах. Предварительно письменно согласовав с БАНКОМ, выпускать рекламную продукцию с торговыми марками МПС.

### **5. ФИНАНСОВЫЕ УСЛОВИЯ**

**5.1.** Взаиморасчеты БАНКА с ТСП производятся в валюте USD - доллар США (наименование валюты), разрешенной законодательством Республики Узбекистан, в порядке и на условиях, определяемых ДОГОВОРОМ.

**5.2.** Факт зачисления/перечисления ТСП денежных средств на основании обработанной АВТОРИЗАЦИИ ТРАНЗАКЦИИ не является безусловным признанием БАНКОМ действительности, проведенной ТСП операции.

**5.3.** ТСП не вправе разбивать стоимость одной покупки (работы, услуги) с проведением двух или более АВТОРИЗАЦИЙ ТРАНЗАКЦИЙ, или принимать альтернативную оплату части стоимости одной покупки (работы, услуги) другими средствами платежа.

**5.4.** За осуществление расчетов по операциям оплаты товаров (работ, услуг) на ИНТЕРНЕТ-ПЛОЩАДКЕ с использованием КАРТ ТСП уплачивает БАНКУ КОМИССИЮ в размере 3%, предусмотренную ТАРИФОМ.

**5.5.** Комиссия, предусмотренная п. 5.4 ДОГОВОРА, взимается каждый раз из суммы возмещения, перечисляемой ТСП БАНКОМ согласно п. 3.1.4 ДОГОВОРА, путем зачета в соответствии с п. 3.2.2 ДОГОВОРА.

### **6. ОТВЕТСТВЕННОСТЬ СТОРОН**

**6.1.** Стороны несут ответственность по ПРАВИЛАМИ ДОГОВОРА в соответствии с законодательством Республики Узбекистан.

**6.2.** В случае неисполнения или ненадлежащего исполнения обязательств по ДОГОВОРУ одной из Сторон, другая Сторона вправе потребовать от виновной Стороны исполнения принятых на себя обязательств, а также возмещения причиненных ей убытков согласно законодательству Республики Узбекистан.

**6.3.** При нарушении БАНКОМ установленного п. 3.1.4 ДОГОВОРА срока перечисления денежных средств БАНК обязуется уплатить ТСП неустойку в размере 0,2 % (Ноль целых две десятых процента) от суммы, подлежащей перечислению, за каждый день просрочки, но не более суммы, не перечисленной в срок.

**6.4.** В случае подтверждения одного из или всех фактов, указанных в п.3.2.6 настоящего ДОГОВОРА, ТСП уплачивает банку пеню в размере 5% от суммы несоответствующего товара (работы, услуги).

**6.5.** ТСП несет ответственность за действия своих работников, связанные с нарушением УСЛОВИЙ ДОГОВОРА, в том числе приложений к нему, если они повлекли неисполнение или ненадлежащее исполнение обязательств ТСП по ДОГОВОРУ.

**6.6.** ТСП несет полную и безоговорочную ответственность за компрометацию данных клиентов и их КАРТ, вызванную хакерскими атаками САЙТА/ИНТЕРНЕТ-ПЛОЩАДКИ(ОК) в связи с невыполнением пунктов 4.1.2, 4.1.6, 4.1.11 и 4.1.12 настоящего ДОГОВОРА и за неверное оформление или совершенной в нарушение правил МПС любой ТРАНЗАКЦИИ. В этом случае, БАНК списывает в бесспорном порядке со счета ТСП средства в размере суммы штрафных санкций, примененных МПС в отношении БАНКА.

**6.7.** БАНК не несет ответственности

- за возможные убытки ТСП, связанные с прекращением проведения АВТОРИЗАЦИИ ТРАНЗАКЦИЙ в случаях, предусмотренных п. 3.2.3 ДОГОВОРА;
- за неверное оформление или совершенной в нарушение правил МПС любой ТРАНЗАКЦИИ.
- по ТРАНЗАКЦИЯМ по скомпрометированным КАРТАМ, в том числе, если установлен или доказан факт, что ТРАНЗАКЦИИ совершены в соответствии со СТАНДАРТАМИ МПС.

## **7. ФОРС-МАЖОР**

**7.1.** Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств по ДОГОВОРУ в случае, если их выполнение оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств, которые возникли после заключения ДОГОВОРА. К таким обстоятельствам Стороны, в частности, но не исключительно, относят: стихийные бедствия, повреждение линий и/или средств связи, введение на территории Республики Узбекистан или отдельных ее местностях военного или чрезвычайного положения, забастовки, принятие органами государственной власти и/или органами местного самоуправления нормативных правовых и иных актов, делающих невозможным исполнение Сторонами своих обязательств по ДОГОВОРУ.

**7.2.** Если любое из обстоятельств, указанных в п. 7.1 ДОГОВОРА, непосредственно повлияло на неисполнение обязательства в срок, указанный в Договоре, то этот срок отодвигается соразмерно на время действия соответствующего обстоятельства и необходимое для устранения его последствий.

**7.3.** Сторона, для которой сделалось невозможным исполнение обязательств вследствие обстоятельств, указанных в п. 7.1 ДОГОВОРА, обязана не позднее 3 (трех) дней с момента их наступления и прекращения в письменной форме уведомить об этом другую Сторону. Извещение должно содержать данные о характере обстоятельств, а также, по возможности, оценку их влияния на возможность исполнения Стороной своих обязательств по ДОГОВОРУ.

**7.4.** Если обстоятельство, препятствующее исполнению обязательств Сторонами, указанное в п. 7.1 ДОГОВОРА, длится более 3 (трех) месяцев, каждая из Сторон вправе отказаться от исполнения ДОГОВОРА в одностороннем порядке путем направления предварительного письменного уведомления другой Стороне. Указанное уведомление должно быть направлено курьером или по почте (с уведомлением о вручении) не позднее, чем за 10 (десять) дней до предполагаемой даты расторжения ДОГОВОРА.

## **8. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА**

**8.1.** Договор вступает в силу с момента его подписания уполномоченными представителями обеих Сторон и действует в течение неопределенного срока.

**8.2.** Каждая из Сторон вправе отказаться от исполнения ДОГОВОРА в одностороннем порядке, письменно уведомив об этом другую Сторону не менее, чем за 30 (тридцать) дней до предполагаемой даты расторжения ДОГОВОРА. Указанное уведомление должно быть направлено курьером или по почте (с уведомлением о вручении).

**8.3.** БАНК прекращает проведение АВТОРИЗАЦИИ ТРАНЗАКЦИЙ с момента направления ТСП или получения от ТСП уведомления о расторжении ДОГОВОРА, предусмотренного п. 8.2 или п. 7.4 ДОГОВОРА.

**8.4.** Расторжение ДОГОВОРА не освобождает Стороны от обязанности провести все взаиморасчеты и платежи по ДОГОВОРУ по операциям, совершенным до даты его расторжения. В случае расторжения ДОГОВОРА, Стороны обязуются произвести все взаиморасчеты и платежи по ДОГОВОРУ в течение 180 (ста восьмидесяти) дней после даты расторжения ДОГОВОРА.

## **9. АНТИКОРУПЦИОННАЯ ОГОВОРКА**

9.1. При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники обязуются не осуществлять, прямо или косвенно, действий, квалифицируемых как дача/получение взятки, коммерческий подкуп, злоупотребление должностным положением, а также действий, нарушающих требования законодательства Республики Узбекистан, международных норм права и международных договоров Республики Узбекистан о противодействии легализации (отмыванию) доходов, полученных преступным путём, и иные коррупционные нарушения – как в отношениях между сторонами Договора, так и в отношениях с третьими лицами и государственными органами. Стороны также обязуются довести это требование до их аффилированных (взаимосвязанных) лиц, работников, уполномоченных представителей и посредников.

9.2. Каждая из сторон Договора, их аффилированные (взаимосвязанные) лица, работники и посредники отказываются от стимулирования каким-либо образом работников или уполномоченных представителей другой стороны, в том числе путем предоставления денежных сумм, подарков, безвозмездного оказания в их адрес услуг или выполнения работ, направленных на обеспечение выполнения этим работником или уполномоченным представителем каких-либо действий в пользу стимулирующей его стороны.

9.3. Под действием работника, осуществляемыми в пользу стимулирующей его стороны понимаются, в том числе:

- а) предоставление неоправданных преимуществ по сравнению с другими контрагентами;
- б) предоставление каких-либо гарантий;
- в) ускорение существующих процедур;

д) иные действия, выполняемые работником в рамках своих должностных обязанностей, но не соответствующие принципам прозрачности и открытости взаимоотношений между сторонами.

9.4. В случае возникновения у Стороны оснований полагать, что произошло или может произойти нарушение другой Стороной, ее аффилированными (взаимосвязанными) лицами, работниками, уполномоченными представителями или посредниками каких-либо обязательств, предусмотренных данной статьей, Сторона обязуется незамедлительно уведомить об этом другую Сторону в письменной форме и по адресу электронной почты, указанной в Договоре. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что такое нарушение произошло или может произойти.

9.5. Сторона, получившая уведомление о нарушении каких-либо положений настоящей статьи, обязана рассмотреть уведомление и сообщить другой стороне об итогах его рассмотрения в течение 10 (десяти) рабочих дней с даты получения письменного уведомления.

9.6. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений настоящей статьи оговорки с соблюдением принципов конфиденциальности и применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны гарантируют отсутствие негативных последствий как для уведомившей стороны в целом, так и для конкретных работников уведомившей стороны, сообщивших о факте нарушений.

9.7. В случае подтверждения факта нарушения одной стороной положений настоящей статьи и/или неполучения другой стороной информации об итогах рассмотрения уведомления о нарушении, другая сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном

порядке путем направления письменного уведомления не позднее чем за 30 (тридцать) календарных дней до даты прекращения действия настоящего Договора.

## 10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Стороны согласны, что источником правового регулирования отношений Сторон в рамках ДОГОВОРА является ДОГОВОР, законодательство Республики Узбекистан, правила, СТАНДАРТЫ и рекомендации МПС, если они не противоречат законодательству Республики Узбекистан. Любые условия и положения ДОГОВОРА, которые противоречат положениям Правил (как известных в момент заключения ДОГОВОРА, так и разработанных в будущем), должны быть приведены в соответствие с правилами.

10.2. Настоящим ТСП предоставляет БАНКУ безотзывное, безусловное, прямое и действительное в течение всего срока действия ДОГОВОРА и дополнительно 6 (шести) календарных месяцев после его прекращения право/распоряжение на списание в бесспорном порядке с любых его счетов, открытых как в БАНКЕ, так и в любом ином БАНКЕ, в любой валюте, средства, причитающиеся БАНКУ, согласно разделу 5 ДОГОВОРА, а также подлежащих возврату ДЕРЖАТЕЛЯМ КАРТОЧЕК, в случаях, указанных в действующем законодательстве, ДОГОВОРЕ, правилах МПС, касающихся предмета ДОГОВОРА.

10.3. Все споры, разногласия или требования, возникающие из ДОГОВОРА или в связи с ним, подлежат урегулированию Сторонами путем переговоров. При отсутствии согласия спор между Сторонами подлежит рассмотрению в Ташкентском межрайонном экономическом суде в соответствии с действующим законодательством Республики Узбекистан.

10.4. Все изменения и дополнения к ДОГОВОРУ действительны лишь в том случае, если они совершены в письменной форме в виде дополнительного соглашения к ДОГОВОРУ и подписаны уполномоченными представителями обеих Сторон.

10.5. Письменные уведомления, предусмотренные в разделе 3 ДОГОВОРА, направляются по факсу или по адресу электронной почты или заказным письмом по адресу, указанному в разделе 10 ДОГОВОРА.

10.6. ДОГОВОР составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон. Приложения и дополнения являются неотъемлемой частью ДОГОВОРА.

10.7. К ДОГОВОРУ на момент его заключения прилагаются:

- Приложение 1: Перечень Интернет-площадок торгово-сервисных предприятий и международных платежных систем, карты которых принимаются к оплате;
- Приложение 2: Правила предоставления услуг электронной коммерции по картам платежных систем через Интернет;
- Приложение 3: Заявление на транзакцию.
- Приложение 4: Перечень запрещенных товаров.
- Приложение 5: Форма о деятельности организации.

## 11. ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН:

БАНК:  
Операционное управление при Главном

ТСП:  
\_\_\_\_\_

управлении НБ ВЭД РУ по городу  
Ташкенту

отделение Национального банка ВЭД РУ

адрес: г. Ташкент, ул. Г. Гуляма, 1,

телефон: (+99871) 244 35 52  
факс: (+99871) 244 35 30  
email: modem@capital.nbu.com

ИНН: 201052966

р/с: \_\_\_\_\_

В  
ОПЕРУ при ТГУ НБ ВЭД РУ

наименование обслуживающего банка

### ПОДПИСИ СТОРОН

От БАНКА:

адрес: \_\_\_\_\_

телефон: \_\_\_\_\_

факс: \_\_\_\_\_

email: \_\_\_\_\_

ИНН: \_\_\_\_\_

р/с: \_\_\_\_\_

В

наименование обслуживающего банка

От ТСП:

***С УСЛОВИЯМИ ДОГОВОРА И  
ПРАВИЛАМИ ОЗНАКОМЛЕН И СОГЛАСЕН***

Управляющий  
Олимжонов К О

\_\_\_\_\_

подпись

Главный бухгалтер в.б  
Юсупов Ш.М.

\_\_\_\_\_

подпись

М.П.

Руководитель

\_\_\_\_\_

ФИО

\_\_\_\_\_

подпись

Главный бухгалтер

\_\_\_\_\_

ФИО

\_\_\_\_\_

подпись

М.П.

Приложение 1 к Договору №\_\_\_\_\_ на  
предоставление услуг электронной  
коммерции по картам международных  
платежных систем через Интернет  
от \_\_\_\_\_ 201\_\_ г.

**ПЕРЕЧЕНЬ САЙТОВ/ИНТЕРНЕТ-ПЛОЩАДОК  
ТОРГОВО-СЕРВИСНЫХ ПРЕДПРИЯТИЙ  
И МЕЖДУНАРОДНЫХ ПЛАТЕЖНЫХ СИСТЕМ,  
КАРТЫ КОТОРЫХ ПРИНИМАЮТСЯ К ОПЛАТЕ**

Наименование САЙТА/ИНТЕРНЕТ-ПЛОЩАДКИ ТСП с указанием адреса и телефона		
НАИМЕНОВАНИЕ МЕЖДУНАРОДНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ, карты которой принимаются к оплате (сделайте отметку системы, с которой вы планируете работать)	<input type="checkbox"/> Visa <input type="checkbox"/> MasterCard <input type="checkbox"/> China UnionPay	<input type="checkbox"/> AMEX <input type="checkbox"/> JCB <input type="checkbox"/> BC Card / Smartro
Официальный САЙТ/ ИНТЕРНЕТ-ПЛОЩАДКА ТСП		

**ПОДПИСИ СТОРОН**

От БАНКА:

Управляющий  
Олимжонов К О

\_\_\_\_\_

подпись

Главный бухгалтер в.б  
Юсупов Ш.М.

\_\_\_\_\_

подпись

М.П.

От ТСП:

Руководитель

\_\_\_\_\_

ФИО

\_\_\_\_\_

подпись

Главный бухгалтер

\_\_\_\_\_

ФИО

\_\_\_\_\_

подпись

М.П.

**ПРАВИЛА  
ПРЕДОСТАВЛЕНИЯ УСЛУГ ЭЛЕКТРОННОЙ КОММЕРЦИИ ПО  
КАРТАМ МЕЖДУНАРОДНЫХ ПЛАТЕЖНЫХ СИСТЕМ  
ЧЕРЕЗ ИНТЕРНЕТ**

**1. Порядок взаимодействия по ДОГОВОРУ на предоставление услуг электронной коммерции по картам МПС.**

- 1.1. Информация о работе в системе ПРОВАЙДЕРА УСЛУГ находится по адресу:  
\_\_\_\_\_.
- 1.2. БАНК совершает необходимые действия для регистрации ИНТЕРНЕТ-ПЛОЩАДКИ в специализированном АПК БАНКА по указанным реквизитам.
- 1.3. ПОКУПАТЕЛЬ через Интернет подключается к САЙТУ/ИНТЕРНЕТ-ПЛОЩАДКЕ, формирует заказ и передает его на дальнейшую обработку специализированному аппаратно-программному комплексу САЙТА/ИНТЕРНЕТ-ПЛОЩАДКИ.
- 1.4. САЙТ/ИНТЕРНЕТ-ПЛОЩАДКА обрабатывает заказ через АПК ПРОВАЙДЕРА УСЛУГ и передает на АПК ПРОВАЙДЕРА УСЛУГ параметры детали и ТРАНЗАКЦИИ, в зависимости от требований ПРОВАЙДЕРА УСЛУГ.
- 1.5. ПОКУПАТЕЛЬ выбирает схему оплаты (3D-Secure, Verified by Visa, MasterCard SecureCode, UCAF, SecurePay, BC Card/Smartro) и в случае необходимости передает на АПК ПРОВАЙДЕРА УСЛУГ информацию о параметрах своей КАРТЫ, включая значения CVC2 или CVV2, дату окончания срока действия карты, персональные данные, что одновременно является подтверждением согласия оплатить заказ.
- 1.6. ПРОВАЙДЕР УСЛУГ проверяет корректность формата вводимых параметров карты ПОКУПАТЕЛЯ и осуществляет дополнительные процедуры аутентификации ПОКУПАТЕЛЯ, в зависимости от поддерживаемой схемы оплаты (3D-Secure, Verified by Visa, MasterCard SecureCode, UCAF, SecurePay, BC Card/Smartro).
- 1.7. При соответствии полученного запроса установленным нормативам, ПРОВАЙДЕР УСЛУГ передает запрос на АВТОРИЗАЦИЮ операции в БАНК.
- 1.8. БАНК проверяет право САЙТА/ИНТЕРНЕТ-ПЛОЩАДКИ провести операцию в соответствии с регистрацией.
- 1.9. БАНК проводит АВТОРИЗАЦИЮ ТРАНЗАКЦИЙ в установленном соответствующими МПС порядке.
- 1.10. При получении БАНКОМ отрицательного результата АВТОРИЗАЦИИ ТРАНЗАКЦИИ, БАНК отправляет уведомление об отказе на АПК ПРОВАЙДЕРА УСЛУГ, который, в свою очередь, передает данную информацию САЙТУ/ИНТЕРНЕТ-ПЛОЩАДКЕ И ПОКУПАТЕЛЮ, с указанием причин отказа.
- 1.11. При положительном результате АВТОРИЗАЦИИ ТРАНЗАКЦИИ БАНК передает на АПК ПРОВАЙДЕРА УСЛУГ подтверждение положительного результата.
- 1.12. АПК ПРОВАЙДЕРА УСЛУГ одновременно передает подтверждения положительного результата проводимой АВТОРИЗАЦИИ операции САЙТУ/ИНТЕРНЕТ-ПЛОЩАДКЕ и ПОКУПАТЕЛЮ.
- 1.13. После получения подтверждения о положительном результате АВТОРИЗАЦИИ операции САЙТ/ИНТЕРНЕТ-ПЛОЩАДКА оказывает услугу (осуществляет работу, отпускает товар) ПОКУПАТЕЛЮ.

1.14. В соответствии с ДОГОВОРОМ, БАНК осуществляет перечисление средств на расчетный счет ТСП в Банке.

1.15. Перечисление средств ТСП осуществляется после обработки БАНКОМ переданного инкассационного пакета АВТОРИЗОВАННЫХ ТРАНЗАКЦИЙ в срок, указанный в п. 3.1.4 ДОГОВОРА.

## **2. Оформление ТРАНЗАКЦИЙ возврата или отмены.**

2.1. Оформление ТРАНЗАКЦИЙ возврата или отмены в стандартных случаях оформляется электронно через персональную страницу ТСП или путем подачи заявления по форме Приложения 3 к ДОГОВОРУ.

## **3. Обработка операций в нестандартных ситуациях**

3.1. В случае, если по техническим или иным причинам (к примеру, ошибка работников ТСП), нет возможности совершить и обработать операцию штатными средствами в соответствии с порядком, изложенным в Договоре, ТСП вправе обратиться в БАНК с просьбой об обработке такой операции (произвести операцию оплаты товара (работы, услуги), возврата, отмены оплаты или отмены возврата) техническими средствами БАНКА.

3.2. Для обработки операции оплаты, отмены оплаты или отмены ранее произведенного возврата ТСП направляет в Банк заявление по форме Приложения 3 к ДОГОВОРУ, а также прилагает все имеющиеся у ТСП чеки, электронные записи и прочие документы, обосновывающие необходимость обработки такой операции. Заявление должно быть подписано лицами, имеющими право подписи в соответствии с карточкой с образцами подписей и оттиска печати, и скреплено оттиском печати ТСП.

3.3. По результатам рассмотрения заявки и прилагаемых документов БАНК вправе осуществить обработку операции, указанной в заявке, или отказать в обработке без объяснения причин; при этом факт зачисления/списания денежных средств по результатам обработки такой операции не является безусловным признанием БАНКОМ действительности данной операции.

## **4. Безопасность платежей**

4.1. Безопасность платежей обеспечивается с помощью АПК БАНКА и АПК ПРОВАЙДЕРА УСЛУГ, функционирующего на основе современных протоколов и технологий, разработанных МПС (3DSecure, UCAF, SecureCode).

4.2. В системе ПРОВАЙДЕРА УСЛУГ безопасность конфиденциальных данных ПОКУПАТЕЛЯ обеспечивается с применением SSL протокола.

4.3. Дальнейшая передача информации осуществляется по закрытым сетям передачи данных, сертифицированным МПС, для доставки конфиденциальной финансовой информации.

4.4. Обработка полученных конфиденциальных данных ПОКУПАТЕЛЯ (реквизиты КАРТЫ, регистрационные данные и т.д.) производится в процессинговом центре.

## **5. Безопасность передаваемой информации**

Безопасность передаваемой информации обеспечивается с помощью современных протоколов обеспечения безопасности в Интернет (SSL/TLS).

## **6. СХЕМА РАБОТЫ по протоколу безопасности 3D-SECURE**

При использовании протокола безопасности 3D-SECURE участвуют четыре стороны:

ТСП должны быть подключены к сервису в рамках программы Verified By Visa или MasterCard SecureCode и разместить бренды «Verified By Visa» и «MasterCard SecureCode» на своих веб-сайтах.

**ЭМИТЕНТЫ** должны использовать Сервера по контролю за доступом (Access Control Server – ACS-Сервер), используемого для аутентификации личности клиента в процессетранзакции, а также управление квитанциями, подписанными электронно.

**ДЕРЖАТЕЛИ КАРТ** Держатели карт должны быть подключены к 3D-Secure. Держатель карты должен ввести пароль и другую информацию о безопасности в процессе аутентификации.

**Сервер Каталога (Directory Server).** МПС, реализаторы 3D-Secure, используют центральный Сервер Каталога, выполняющий роль домена взаимодействия для идентификационной информации и адресов ACS-серверов эмитентов-участников сервисов в рамках программ Verified By Visa и MasterCard SecureCode.

#### 6.1. Аутентификация участников платежа

Технология проведения платежей за товары и услуги в сети Интернет, поддерживаемая в рамках проекта, базируется на текущих спецификациях МПС, таких как Visa (спецификация Visa 3D-Secure, название маркетинговой программы – Verified by Visa) и MasterCard (спецификация SPA/UCAF, название маркетинговой программы – MasterCard SecureCode).

С целью обеспечения необходимого уровня безопасности, предотвращения мошеннических операций и финансовых потерь участников электронных сделок в Интернете обе спецификации базируются на одном и том же основополагающем принципе – взаимной аутентификации участников платежа. Реализован этот принцип с использованием модели трех доменов (см. рис.1.).

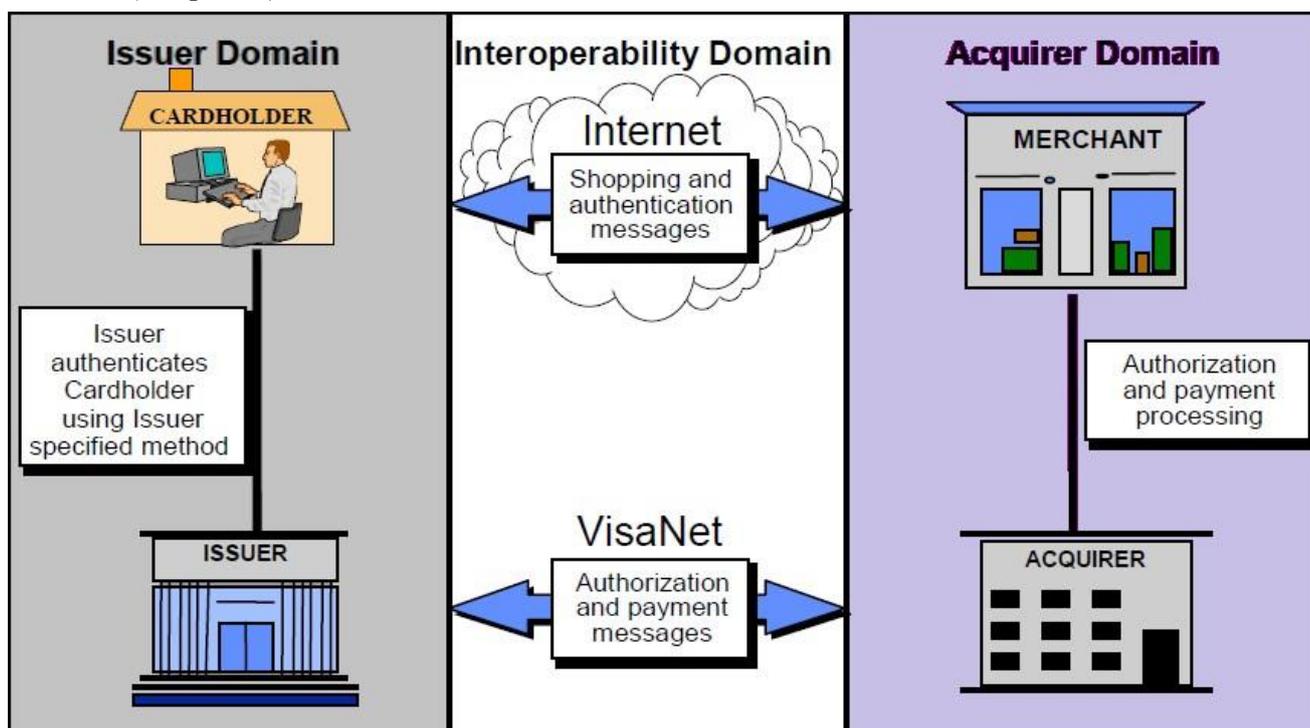


Рис.1. Реализация аутентификации по протоколу 3D-Secure использованием модели трех доменов

Назначение каждого из упомянутых доменов следующее:

**Домен эмитента (Issuer domain)** – его назначение заключается в том, что перед тем как выполнить авторизацию, т.е. проверку платежеспособности карты, банк-эмитент, выпустивший данную карту, производит аутентификацию покупателя – держателя этой карты, тем самым подтверждая подлинность личности покупателя. В итоге – вся ответственность за аутентификацию и за подлинность транзакции в целом ложиться на банк-эмитент.

**Домен эквайера (Acquirer domain)** – его назначение заключается в том, что обслуживающий банк производит аутентификацию своей торговой точки на основе правил и методов, установленных самим обслуживающим банком (т. е. в этом случае вся

ответственность за аутентификацию электронного магазина ложится на обслуживающий торговую точку банк).

**Домен взаимодействия** (Interoperability domain) – его назначение в том, чтобы определить правила и процедуры обмена информацией между доменами ЭМИТЕНТА и ЭКВАЙЕРА, гарантирующие этим доменам взаимную аутентификацию друг друга. Указанный домен поддерживается самой МПС.

Держатель карты находится в домене эмитента, а предприятие торговли и сервиса находится в домене эквайера, которые в свою очередь взаимодействуют между собой через домен взаимодействия.

Таким образом, модель трех доменов (3D), разбивая процесс аутентификации участников транзакции на отдельные зоны, сразу ограничивает множество всех протоколов электронной коммерции, определяя лишь некоторое подмножество всех возможных алгоритмов взаимодействия участников транзакции.

Также следует заметить, что процедуры аутентификации внутри доменов ЭМИТЕНТА и ЭКВАЙЕРА определяются соответственно банком-эмитентом и банком- эквайером. МПС определяет лишь правила работы в домене Interoperability Domain, через который, как было отмечено выше, происходит взаимодействие между клиентом и торговой точкой. То сеть модель трех доменов ясно определяет ответственность всех участников транзакции в процессе их аутентификации (своего рода делегирование).

Главным и очевидным преимуществом рассматриваемой модели является, то, что ЭМИТЕНТ получает возможность производить аутентификацию своего клиента любым удобным ему способом.

## **6.2. ОПИСАНИЕ ТЕХНОЛОГИИ ПЛАТЕЖЕЙ**

(на примере обслуживания карт Visa)

Для осуществления платежей по технологии 3D-Secure ДЕРЖАТЕЛЬ КАРТЫ может быть дополнительно аутентифицирован посредством привязки его международной КАРТЫ к мобильному телефону, то есть стать участником программы Verified by Visa.

Во время совершения транзакции в сети Интернет, магазин, передавая централизованному ресурсу (платежному серверу ЭКВАЙЕРА) основные параметры транзакции, инициирует связь платежного сервера со специальной системой Visa с целью проверки, является ли держатель карты участником указанной выше программы.

В случае утвердительного ответа, ЭМИТЕНТУ направляется запрос на аутентификацию ДЕРЖАТЕЛЯ КАРТЫ. Этот запрос передается эмитенту в виде строки параметров, присоединенной к web-адресу системы аутентификации банка-эмитента (параметры передаются в браузер самого покупателя). Тем самым покупатель переадресуется на систему аутентификации своего ЭМИТЕНТА.

Во время совершения ТРАНЗАКЦИИ клиенту на его мобильный телефон направляется SMS-сообщение, содержащее код аутентификации, при этом клиент попадает на специальную web-страницу, защищенную протоколом шифрования SSL, где от него требуется ввести полученный код (аутентифицироваться).

После подтверждения личности ДЕРЖАТЕЛЯ КАРТЫ система аутентификации ЭМИТЕНТА генерирует специальное уникальное цифровое значение, играющее роль подписи, удостоверяющей данную сделку. Эта подпись передается платежному серверу и затем становится частью авторизационного запроса, который магазин (платежный сервер) направляет своему ЭКВАЙЕРУ, а тот, в свою очередь, направляет авторизационный запрос банку-эмитенту. Проверив подпись и убедившись в платежеспособности карты, ЭМИТЕНТ завершает (одобряет) транзакцию. Таким образом, ЭМИТЕНТ аутентифицирует держателя карты в момент проведения платежа и уведомляет виртуальный магазин в режиме реального времени о том, действительно ли покупатель является владельцем карты.

Благодаря этой схеме расчеты по международным картам Visa будут защищены от такого явления, как потребительские споры и отказы от совершения сделки.

Отдельные этапы осуществления платежа в Интернете проиллюстрированы на рис.2.

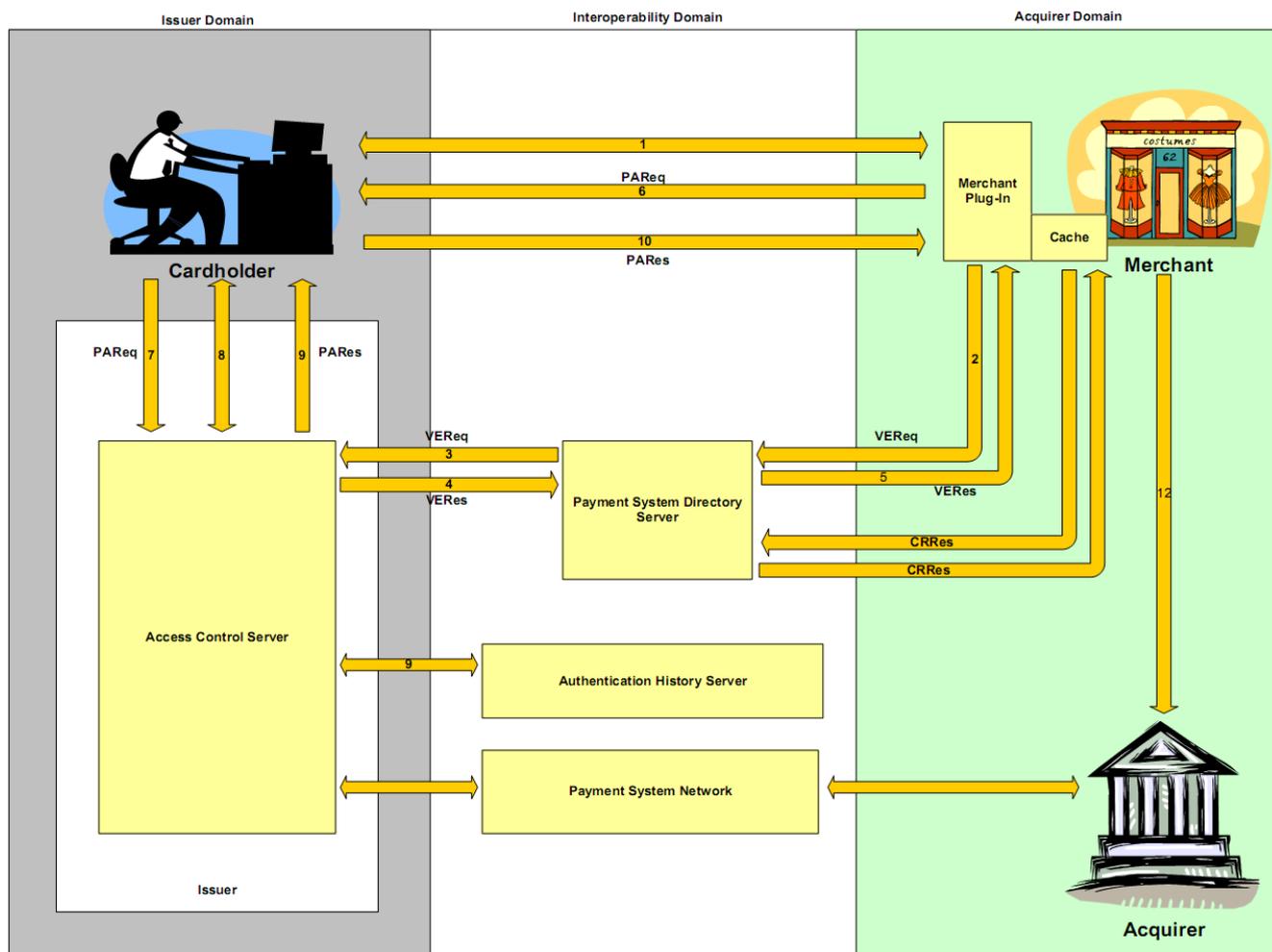


Рис. 2. Трехдоменная схема осуществления платежа в Интернете, с разбиением на этапы этап

1. Покупатель выбирает необходимые товары в электронном Интернет-магазине ТСП и формирует «корзину» заказа.
  - этап 2. Дополнительный программный модуль Merchant Plug-In (MPI) генерирует запрос на проверку регистрации (VEReq) на сервер МПС для определения доступности аутентификации данной конкретной карты.
  - этап 3. Если номер карты участвует в сервисе 3D-Secure, Сервер Каталога запрашивает соответствующий ACS-Сервер, чтобы определить, зарегистрирована ли в нем карта. (В противном случае, создается ответ о проверке регистрации (VeRes) для модуля MPI и обработка продолжается с этапа 5).
- Ответ VeRes отправляется Сервером Каталога в модуль MPI, с извещением модуля MPI, что аутентификация недоступна для данной карты. Ответ VeRes также может быть направлен от ACS-Сервера через Сервер Каталога, как описано в этапах 4 и 5, если сервер определит, что номер карты, действительно относится в участвующему диапазону карт и пересылает запрос к соответствующему ACS-Серверу.
- этап 4. ACS-Сервер отвечает Серверу Каталога с ответом VERes, отмечая, доступна ли аутентификация для номера карты.
  - этап 5. Сервер Каталога перенаправляет ответ VERes ACS-сервера или свой собственный ответ VERes в модуль MPI в случае обнаружения, что карта не входит в

участвующий диапазон номеров карт. Если ДЕРЖАТЕЛЬ КАРТЫ не зарегистрирован в 3D-Secure или в ином случае аутентификация недоступна, после предоставляется обычный запрос на авторизацию и процесс завершается.

этап 6. Модуль MPI посылает запрос на аутентификацию плательщика (PAREq) для ACS-Сервера с помощью браузера покупателя, предоставляя данные, необходимые для попытки аутентификации ДЕРЖАТЕЛЯ КАРТЫ.

этап 7. ACS-Сервер получает запрос PAREq.

этап 8. ACS-Сервер аутентифицирует покупателя как соответствующего для номера карты (включая использование методов, таких как пароль, чиповая криптограмма или ПИН), затем форматирует сообщение ответа на аутентификацию плательщика (PAREs) с соответствующими значениями и ставит цифровую подпись. PAREs отмечает была ли аутентификация успешной или нет.

этап 9. ACS-Сервер возвращает ответ PAREs в модуль MPI через браузер покупателя. ACS-Сервер направляет копию ответа PAREs в Сервер историй аутентификации (Authentication History Server). Сервер историй аутентификации является компонентом, работающим в домене взаимосвязи (Interoperability Domain); архивирует деятельность, используемую ЭКВАЙЕРАМИ и ЭМИТЕНТАМИ для разрешения споров и других целей.

этап 10. Модуль MPI получает ответ PAREs.

этап 11. Модуль MPI подтверждает подпись ответа PAREs (или производя подтверждение самостоятельно или передавая сообщение на отдельный Сервер подтверждения (Validation Server)).

этап 12. ТСП осуществляет обмен авторизацией с со своим ЭКВАЙЕРОМ.

Следуя этапу 12, ЭКВАЙЕР процессирует АВТОРИЗАЦИЮ с ЭМИТЕНТОМ через сеть МПС и возвращает результат ТСП.

### **6.3. ВОПРОСЫ БЕЗОПАСНОСТИ**

1. Применяемый способ АВТОРИЗАЦИИ гарантирует Покупателю, что платежные реквизиты его карточки (номер, срок действия, CVV2/CVC2) не попадут в руки мошенников, так как эти данные не хранятся на торговом сервере Интернет-ТСП и, следовательно, не могут быть оттуда похищены.
2. Покупатель вводит свои платежные реквизиты не на сайте интернет-магазина, а непосредственно в процессинговом центре на защищенной странице платежного сервера, следовательно, платежные реквизиты КАРТОЧКИ Покупателя не будут доступны персоналу ТСП. Данная функциональность является реализацией требований по безопасности МПС для ТРАНЗАКЦИЙ электронной коммерции.
3. Безопасность передаваемых данных обеспечивается использованием протокола SSL и поэтому они не могут быть перехвачены в момент передачи по каналам связи.
4. Информация о реквизитах КАРТЫ, сохраняемая для последующей обработки в БД процессингового центра подвергается дополнительному шифрованию и может быть прочитана только уполномоченным персоналом.
5. Безопасность обмена платежной информацией между Интернет-магазином и платежным сервером обеспечивается использованием механизма MAC-подписи, что исключает возможность искажения передаваемой информации при передаче ее через браузер Покупателя.

### **7. Требования к разработке ИНТЕРНЕТ сайта ТСП. Политика возврата товара, обратной связи и подтверждения клиентом получения товара.**

- 7.1 При разработке интернет сайта, ТСП обязан учесть минимальные требования банка. К таким требованиям относиться следующие:
  - Разработать политику возврата товара и обратной связи на сайте, с указанием

ответственных лиц.

- Указать на сайте электронный адрес (email) банка для жалоб покупателей в случае несанкционированного списания.
- Инструмент для отслеживания доставки товара.
- Ссылка для подачи заявки на возврат товара и средств.
- Торговая точка должна поддерживать возможность запроса кода 3D Secure с плательщика.
- Необходим тайм-аут аккаунта пользователя (плательщика). В случае бездействия на протяжении 15 минут (время на рассмотрение)
- Рассмотреть такую возможность: При регистрации (или в какой-нибудь другой “рабочий момент”) пользователя к реквизитам Visa карты зафиксировать мобильный номер. Для того, чтобы при осуществлении транзакции с данной карты сайт запрашивает смс с данного мобильного номера.

7.2 ТСП на своем интернет сайте должен хранить все детали транзакции в течении 6 месяцев, и по первому требованию банка предоставить всю необходимую информацию в обслуживающие отделения или филиал. Детали транзакции должны содержать следующую информацию.

- Ф.И.О покупателя.
- Наименования товара и количество.
- Дата и время транзакции.
- С какого IP адреса прошла авторизация и покупка.
- Цена товара.
- Адрес покупателя, электронная почта и телефон.
- Номер заказа.
- Прикрепленный мобильный номер с смс подтверждением.

Приложение 3 к Договору № \_\_\_\_\_  
на предоставление услуг электронной  
коммерции по картам международных  
платежных систем через Интернет  
от \_\_\_\_\_ 201\_\_ г.

### ЗАЯВЛЕНИЕ НА ОПЕРАЦИЮ

\_\_\_\_\_ (наименование ТСП и сайта/Интернет-площадки)

Расходная  Частичная  Полная  Возврат<sup>2</sup>  
Операция<sup>1</sup> отмена<sup>2</sup> отмена<sup>2</sup>

Руководителю \_\_\_\_\_ отделения Национального банка ВЭД РУ

I. Поручение о списании, частичной/полной отмене, возврате средств (ненужное вычеркнуть)

Наименование платежной системы	
Дата оплаты заказа	
Время оплаты заказа	
Сумма заказа	
Номер заказа	
Код терминала	
Код авторизации	
4 последние цифры номера карты покупателя	
Сумма транзакции (цифрами и прописью):	

От ТСП:

Руководитель

\_\_\_\_\_ подпись \_\_\_\_\_ ФИО

Главный бухгалтер

\_\_\_\_\_ подпись \_\_\_\_\_ ФИО

М.П.

« \_\_\_\_ » \_\_\_\_\_ 201\_\_ г.

<sup>1</sup> Оформляется в случае отсутствия технической возможности самостоятельно выполнить операцию или в нестандартных случаях

<sup>2</sup> Может быть оформлено ТСП как в стандартных, так и нестандартных случаях.

При оформлении заявки на частичную/полную отмену или возврат операции заполняется вторая часть после подсчета общего количества подлежащих отмене/возврату транзакций.

II. Произвести полную/частичную отмену операции; отмену операции возврата, спрoцессировать операцию и т.п. (ненужное вычеркнуть)

Количество отмененных/возвратных транзакций:	
Общая сумма цифрами прописью:	
Номер инкассированного пакета	
Общая сумма инкассированного пакета цифрами прописью:	

« \_\_\_\_ » \_\_\_\_\_ 201\_\_ г.

От ТСП:

Руководитель

\_\_\_\_\_                      \_\_\_\_\_  
подпись                      ФИО

Главный бухгалтер

\_\_\_\_\_                      \_\_\_\_\_  
подпись                      ФИО

М.П.

« \_\_\_\_ » \_\_\_\_\_ 201\_\_ г.

Приложение 4 к Договору № \_\_\_\_\_  
на предоставление услуг электронной  
коммерции по картам международных  
платежных систем через Интернет  
от \_\_\_\_\_ 201\_\_ г.

## **ПЕРЕЧЕНЬ ЗАПРЕЩЕННЫХ ТОВАРОВ**

- Товары и/или услуги эротического и порнографического характера.
- Алкогольная и спиртосодержащая продукция (включая слабоалкогольные напитки)
- Табак и табачные изделия.
- Лицензируемые виды деятельности, без наличные действующих лицензий и/или специальных разрешений.
- Агентская деятельность без наличия прямых договоров с производителями/поставщиками.
- Лекарственные средства и медицинские препараты, биологически активные добавки (БАД).
- Исторические и культурные ценности, музейные экспонаты.
- Запрещенные, действующим законодательством наркотические и психотропные вещества.
- Товары, являющиеся полными или частичными копиями товаров зарегистрированных товарных марок, без обязательного указания на веб-сайте (а также на самих товарах) того, что это копии.
- Благотворительность, взносы, пожертвования без соответствующих лицензий (регистрации).
- Продажа цифровых товаров без наличия договоров с поставщиками (дистрибьюторами) и/или и правообладателями.
- Все виды азартных игр, (за исключением официально зарегистрированных лотерей, в соответствии с законодательством).
- Продажи и распространение продукции и материалов, пропагандирующих насилие, межнациональную рознь, терроризм и экстремистскую деятельность.
- Товары и/или услуги, противоречащие действующему законодательству или в отношении, которых действуют ограничения или иные правила торговли.
- Платёжные системы, и/или агрегаторы платежных средств для торгово-сервисных предприятий, предоставляющие услуги оплаты в пользу третьих лиц, пополнения собственного «виртуального» счета с последующим расходованием средств на товары/услуги третьих лиц, обмена и/или конвертации зачисленных денежных средств, электронных валют, а также вывод и/или обналичивания денежных средств с «виртуального» счета.

Приложение 5 к Договору № \_\_\_\_\_  
на предоставление услуг электронной  
коммерции по картам международных  
платежных систем через Интернет  
от \_\_\_\_\_ 201\_\_ г.

**Merchant application form.**  
**Форма о деятельности организации.**

<b>Corporation details. Данные организации.</b>	
Company Name Наименование организации.	
Registered address Юридический адрес	
Post code and city Индекс и город	
Contact Person name, phone and email. Контактное лицо, имя, телефон и почта.	
<b>Bank account information – Данные банковского счета</b>	
Main Account Основной счет	
Bank name Банк	
Account number Номер счета	
Bank branch МФО	
Swift code Свифт	
<b>Website details – Данные вэб сайта</b>	
Website name Наименования вэб сайта	
Type of business Вид деятельности	
IP Address IP Адрес	
Customer Support email Электронный адрес службы поддержки клиентов	
Chargeback notification email. Электронный адрес по спорным ситуациям.	
How long have you been in business? Сколько времени вы занимаетесь этим видом деятельности?	
Currently monthly sales volume. Текущий объем за месяц.	

Current number of monthly transaction. Текущее количество транзакции за месяц.	
How do you receive your customer's order? Где вы получаете свои заказы?	Internet _____ (%) Telephone order _____ (%)
SSL certificate, when, where and expire date. SSL сертификат, когда и кем получен, и срок действительности	
Technical contact name of web site, phone and email. Контактное техническое лицо по администрированию вэб сайта, телефон и Эл. почта	
<b>Website content / Наименования продукта/товаров.</b>	
What is/ are the product/s or services sold on your website? Какие виды товаров\услуг реализуются на Вашем вэб сайте?	
Min / average / max price of goods / services on the site Мин/сред/макс цена товаров/услуг на сайте.	
Describe the terms of delivery of goods, and the terms of the service. Опишите условия доставки товара, или условия оказания услуги.	
Describe the terms of return policy or cancel services. Опишите условия возврата товара или отмена услуги	
Do you send an email receipt to the cardholder when the product delivered? Describe for example. Вы отправляете оповещение клиенту, когда товар был доставлен. Приведите пример.	