ПРИЛОЖЕНИЕ № 14
к Соглашению комплексного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АКБ «Капиталбанк»

ПОРЯДОК
на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет

I. ДОПОЛНИТЕЛЬНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ:

1.1. В настоящем Порядке используются следующие термины и определения:

Авторизация – процедура запроса и последующего получения ТСП от МПС 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 МПС 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 Банка.

Интернет-площадка – Интернет-ресурс ТСП или его партнеров, включающий в себя Сайт в сети Интернет, позволяющий ТСП принимать и обслуживать заказы на приобретение товаров (работ, услуг) через Интернет.

Карта – банковская платежная карта, эмитированная Эмитентом его Держателю (владелец счета международной карты) под эгидой МПС.

Транзакция – безналичная операция в иностранной валюте, совершаемая Держателем (владельцем счета Международной карты) при помощи Карты, с обязательным проведением Авторизации.

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 (3DSecure, Verified by Visa, MasterCard SecureCode, UCAF, SecurePay, BC Card/Smartro).

Правила – руководство по предоставлению Услуг ТСП, которые являются неотъемлемой частью настоящего Порядка.

Услуги – услуги электронной коммерции по картам МПС, оказываемые 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, который является обязательным для применения ТСП.

1.2. Иные термины и определения, используемые в настоящем Порядке, имеют то же значение, что и в Соглашении.

II. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Порядок становится обязательным для Сторон (вступает в силу) на основании подписанного собственноручно (в бумажной форме) или ЭЦП (в электронной по системе IBK) Клиентом Заявления на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет (далее – «Заявление») и регулирует взаимоотношения между Банком и Клиентом в связи с реализацией Клиентом товаров (работ, услуг) на Сайте или Интернет-площадке с приемом оплаты посредством использования Карты и организацией Банком проведения таких Транзакций с применением АПК для перечисления на счета Клиента денежных средств.

2.2. Настоящий Порядок, Соглашение, Тарифы Банка, а также Заявление, в совокупности составляют Договор на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет VISA (далее – «Договор»).

III. ПРАВА И ОБЯЗАННОСТИ БАНКА

3.1. Банк обязуется:

3.1.1. обеспечить Клиенту предоставление доступа к АПК для проведения операций по оплате товаров (работ, услуг) на Сайте или Интернет-площадке с использованием Карт;

3.1.2. организовать с применением АПК, указанного в п. 3.1.1. настоящего Порядка, проведение Транзакций, осуществляемых с использованием Карт на Сайте или Интернет-площадке, в круглосуточном режиме (24/7);

3.1.3. организовать прием от Клиента и обработку авторизованных Транзакций, проведенных законными держателями Карт;

3.1.4. осуществлять перечисление денежных средств, оплаченных посредством Карт на расчетный счет ТСП согласно Тарифов Банка, на расчетный счет Клиента в течение 5 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. настоящего Порядка;

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 (работ, услуг) Картой на Сайте или Интернет-площадке.

3.2. Банк вправе:

3.2.1. 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 комиссий и выставлений (таких как «Chargeback» и «Representment», «Pre-Compliance», «Pre-Arbitration»), которые были получены от МПС по данному ТСП;

3.2.2. в одностороннем порядке прекратить проведение Авторизации Транзакций при нарушении Клиентом согласно Приложению 2 к настоящему Порядку, а также обязанности, приведённые в пунктах и подпунктах раздела 4 настоящего Порядка;

3.2.3. направить Клиенту в течение 2 (двух) рабочих дней соответствующее письменное уведомление о прекращении Авторизации Транзакций;

3.2.4. проводить совместный с МПС и/или Клиентом/односторонний плановый/внеплановый аудит Клиента на предмет выявления мошеннических операций с Картами, предоставления Клиентом покупателям несогласованных с Банком товаров (работ, услуг) и подставных Сайтов или Интернет-площадок;

3.2.6. незамедлительно блокировать все Авторизации, если установлены факты, что реализуемые товары (работы, услуги) на Сайте или Интернет-площадке не соответствуют заявленной деятельности, и/или присутствуют в списке запрещенных товаров согласно Приложению 4 к настоящему Порядку и/или Сайт/Интернет-площадка занимается незаконными действиями, в том числе обналичиванием и/или отмыванием денежных средств;

3.2.7. не возмещать Клиенту денежные средства при возникновении спорных ситуаций, если Банк получил «Fraud Report» (отчет о мошенничестве) или «Chargeback» / «Finance Dispute» (отказ от Транзакции) / «representment» (повторный отказ от Транзакции) по проведенным Транзакциям до выяснения всех обстоятельств, которые по правилам МПС могут составлять от одного до четырех месяцев;

3.2.8. приостановить зачисление (замораживание) денежных средств на счет Клиента до полной проверки подозрительных Транзакций, которые попали в программу мониторинга «FraudGuard» или «Visa Fraud Monitoring Program», направив запрос в Эмитент;

3.2.9. вернуть денежные средства банкам-эмитентам при выявлении МПС в Транзакциях Клиента подозрительную активность и заведении дела по защите брэнда, или при превышении порогового лимита по программе мониторинга подозрительных Транзакций МПС;

3.2.10. оставить за собой право проводить Авторизации с Карт, у которых не поддерживается «3D Secure» Авторизации;

3.2.11. в одностороннем порядке приостановить действие Договора и отказать в осуществлении операции с денежными средствами в случае, если:

- Клиентом предоставлены заведомо недостоверные документы или не представлены документы, запрашиваемые, Банком в соответствии с законодательством, об идентификации Клиента, об источниках происхождения денежных средств и (или) иного имущества Клиента;

- у Банка имеются обоснованные подозрения, что использование Договора Клиентом и/или Бенефициарным собственником осуществляется в целях легализации доходов, полученных от преступной деятельности, и финансированию терроризма;

- у Банка имеются сведения об участии или подозрении в участии Клиента в террористической или иной преступной деятельности, полученных в соответствии с действующим законодательством Республики Узбекистан;

- наложения ареста на денежные средства Клиента, находящиеся на счете, или приостановления операций по счету в случаях, предусмотренных законодательством Республики Узбекистан;

3.2.12. в порядке, установленном законодательством Республики Узбекистан и локальными актами АКБ «Капиталбанк» без согласия Клиента осуществить замораживание и/или приостановление операций с денежными средствами или иным имуществом (за исключением операций по зачислению денежных средств) в случаях, когда в соответствии с действующим законодательством лица подпадают в Перечень лиц. В случае приостановления операции и (или) замораживании денежных средств и иного имущества списание денежных средств со счетов Клиента не производится;

3.2.13. приостановить предоставление Услуги в случае отсутствие связи с МПС.

3.3. Стороны могут иметь иные права и обязанности, предусмотренные законодательством Республики Узбекистан и Соглашением.

IV. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

4.1. Клиент обязуется:

4.1.1. исполнять Правила, указанные в Приложении 2 к настоящему Порядку;

4.1.2. обеспечить предоставить актуальный сертификат 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 Держателем (владельцем счета международной карты) 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 и/или МПС до передачи инкассированного пакета Транзакций;

- Транзакции возврата – электронно или в виде «Формы заявки о возврате средств» согласно Приложению 3 к настоящему Порядку, в том числе при невозможности оформления Транзакции отмены;

4.1.5. разместить на Сайте информацию, касающуюся обеспечения конфиденциальности данных покупателей и обеспечения безопасности платежей в соответствии с разделами 4, 5 Приложения 2 к настоящему Порядку, а также разделами, регламентирующими вопросы безопасности и порядок борьбы с мошенничеством на Сайте Банка;

4.1.6. 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;

4.1.7. согласовывать с Банком дизайн платежной страницы Сайта или Интернет-площадки(ок), включая электронные варианты рекламных наклеек с логотипом МПС, указанных в Приложении 1 к настоящему Порядку;

4.1.8. в обязательном порядке предоставить в Банк следующую информацию:

- о перечне товаров (работ, услуг), предоставляемых Сайтом или Интернет-площадкой(ами) покупателям с указанием мин/сред/макс цены каждого товара (работ, услуг), квитанции почтовых служб об отправке товара (работ, услуг);

- о доменном имени Сайта или Интернет-площадки(ок) и о любых его изменениях;

- информацию о IP-адресах, с которых осуществлена Транзакция, Сайта или Интернет-площадки(ок) и о любых их изменениях;

4.1.9. не реализовывать товары (работы, услуги), запрещенные к продаже/предоставлению согласно законодательству Республики Узбекистан. Перечень запрещенных товаров (работ, услуг) приведен в Приложении 4 к настоящему Порядку;

4.1.10. предоставить Банку и/или в МПС постоянный доступ к электронным журналам и/или базам данных регистрации операций каждого Сайта или Интернет-площадки;

4.1.11. а 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);

4.1.12. на регулярной основе осуществлять проверку Сайт или Интернет-площадки 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);

4.1.13. 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;

4.1.14. хранить банковскую и коммерческую тайны Банка и держателей Карт, ставшие известными ТСП в результате выполнения условий Договора;

4.1.15. предоставить заполненную Форму о деятельности организации приведенной в Приложении 5 к настоящему Порядку.

4.2. Клиент вправе:

4.2.1. требовать от Банка своевременного зачисления сумм в соответствии с пунктом 3.1.4 (за исключением случаев по пунктам 3.2.7 – 3.2.8 и 3.2.9 настоящего Порядка) операций по оплате товаров (работ, услуг), совершенных с использованием Карт на Сайте или 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.

4.3. Стороны могут иметь иные права и обязанности, предусмотренные законодательством Республики Узбекистан и Соглашением.

V. ФИНАНСОВЫЕ УСЛОВИЯ

5.1. Взаиморасчеты Банка с Клиентом производятся в долларах США, в соответствии с законодательством Республики Узбекистан, в порядке и на условиях, определяемых Договором.

5.2. Факт зачисления/перечисления Клиентом денежных средств на основании обработанной Авторизации Транзакции не является безусловным признанием Банком действительности, проведенной Клиентом операции.

5.3. Клиент 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 Сайте или Интернет-площадке с использованием Карт взимаются издержки или комиссии Поставщиков услуг МПС Клиента в указанном размере Тарифе Банка каждый раз из суммы возмещения.

VI. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнения своих обязательств по Договору в соответствии с действующим законодательством Республики Узбекистан, Соглашением и настоящим Порядком.

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.

6.3. При нарушении Банком установленного п. 3.1.4. настоящего Порядка срока перечисления денежных средств, Банк обязуется уплатить Клиенту пеню в размере 0,1 % (Ноль целых одна десятых процента) от суммы, подлежащей перечислению, за каждый день просрочки, но не более 50% (Пятьдесят процентов) от суммы, не перечисленной в срок.

6.4. В случае подтверждения одного из или всех фактов, указанных в п.3.2.6 настоящего Порядка, Клиент уплачивает Банку штраф в размере 5% от суммы несоответствующего товара (работы, услуги).

6.5. Клиент 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 Клиента по Договору.

6.6. Клиент несет полную и безоговорочную ответственность за компрометацию данных клиентов и их КАРТ, вызванную хакерскими атаками Сайта и Интернет-площадки(ок), в том числе в связи с невыполнением пунктов 4.1.2, 4.1.5, 4.1.10 и 4.1.11 настоящего Порядка и за неверное оформление или совершенной в нарушение правил МПС любой Транзакции. В этом случае, Банк списывает в бесспорном порядке со счета Клиента средства в размере суммы штрафных санкций, примененных МПС в отношении Банка.

6.7. БАНК не несет ответственности:

- за возможные убытки Клиента, связанные с прекращением проведения Авторизации Транзакций в случаях, предусмотренных п. 3.2.3 настоящего Порядка;
- 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;
- если исполнение обязательств Банка по Договору зависит от определенных действий третьих лиц и/или Поставщика услуг МПС, или невыполнение или несвоевременное выполнение связано с тем, что третье лица и/или Поставщик услуг не могут или отказываются совершить необходимые действия либо совершают их с нарушениями установленного порядка.

VII. ЗАКЛЮЧИТЕЛЬНЫЕ УСЛОВИЯ

7.1. Договор вступает в силу с момента подачи Клиентом Заявки и действует до полного исполнения сторонами своих обязательств.

7.2. При расторжении Договора, оплаченные комиссионные вознаграждения Банку согласно Тарифу Банка, Клиенту возврату не подлежат.

7.3. Споры, связанные с Договором, решаются сторонами путем переговоров между собой. В случае невозможности разрешения споров путем переговоров, споры решаются в порядке, оговоренном Соглашении.

7.4. Отношения между Банком и Клиентом, не предусмотренные настоящим Порядком, регулируются действующим законодательством Республики Узбекистан и Соглашением.

7.5. Стороны согласны, что источником правового регулирования отношений Сторон в рамках Договора является сам Договор, Действующее законодательство, 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.

Приложение № 1
к Порядку на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет

ПЕРЕЧЕНЬ
сайтов/интернет-площадок торгово-сервисных предприятий и международных платежных систем, карты которых принимаются к оплате

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

ПОДПИСИ СТОРОН

От Банка:

Управляющий

_____
ФИО

_____
подпись

Главный бухгалтер

_____ ФИО

_____
подпись

М.П.

От Клиента:

Руководитель

_____
ФИО

_____
подпись

Главный бухгалтер

_____
ФИО

_____
подпись

М.П.

Приложение № 2
к Порядку на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет

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 ПОСТАВЩИКА УСЛУГ МПС 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 ПОСТАВЩИКА УСЛУГ МПС параметры детали и ТРАНЗАКЦИИ, в зависимости от требований ПОСТАВЩИКА УСЛУГ МПС.

   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 ПОСТАВЩИКА УСЛУГ МПС 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. ПОСТАВЩИК УСЛУГ МПС 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, ПОСТАВЩИК УСЛУГ МПС 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 ПОСТАВЩИКА УСЛУГ МПС, 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 ПОСТАВЩИКА УСЛУГ МПС подтверждение положительного результата.

   1.12. АПК ПОСТАВЩИКА УСЛУГ МПС 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 ПОСТАВЩИКА УСЛУГ МПС, функционирующего на основе современных протоколов и технологий, разработанных МПС (3DSecure, UCAF, SecureCode).

4.2. В системе ПОСТАВЩИКА УСЛУГ МПС 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 процессе транзакции, а также управление квитанциями, подписанными электронно.

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.).

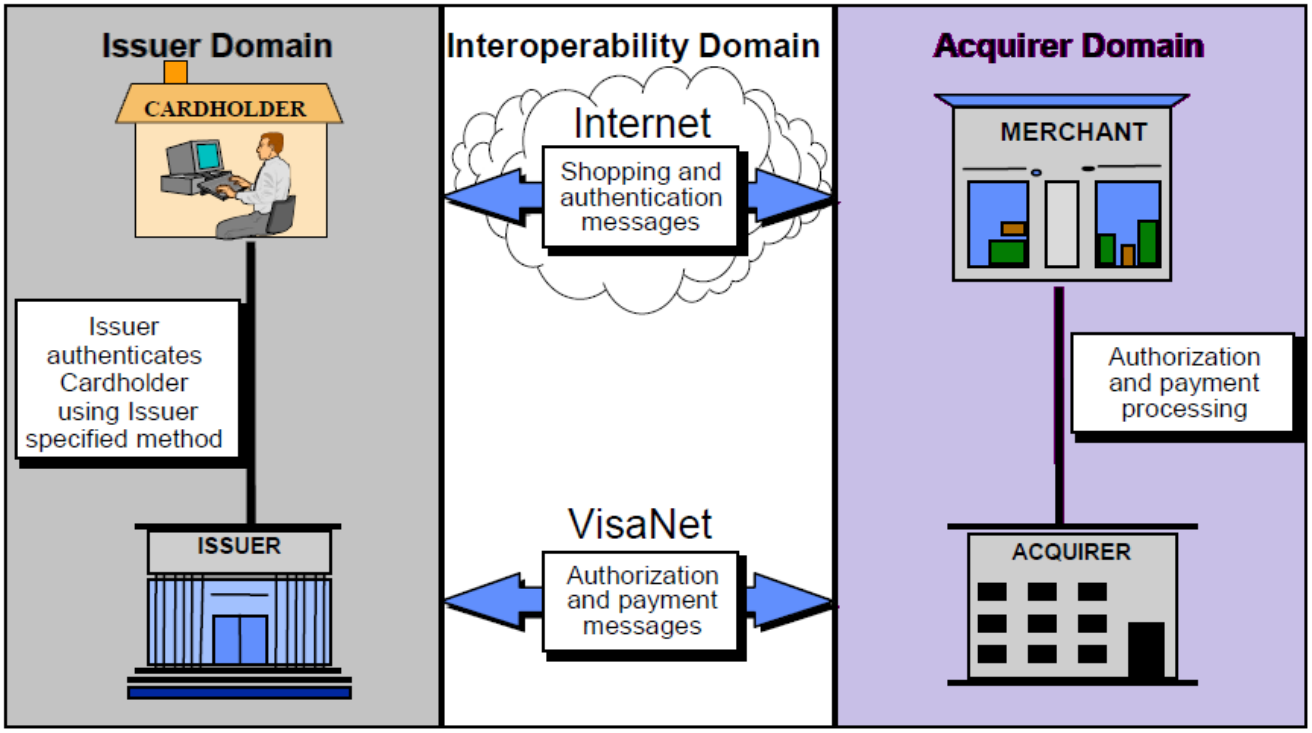

Рис.1. Реализация аутентификации по протоколу 3D-Secure использованием модели трех доменов

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 ЭКВАЙРЕРА) 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 ЭКВАЙРЕРУ, 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.

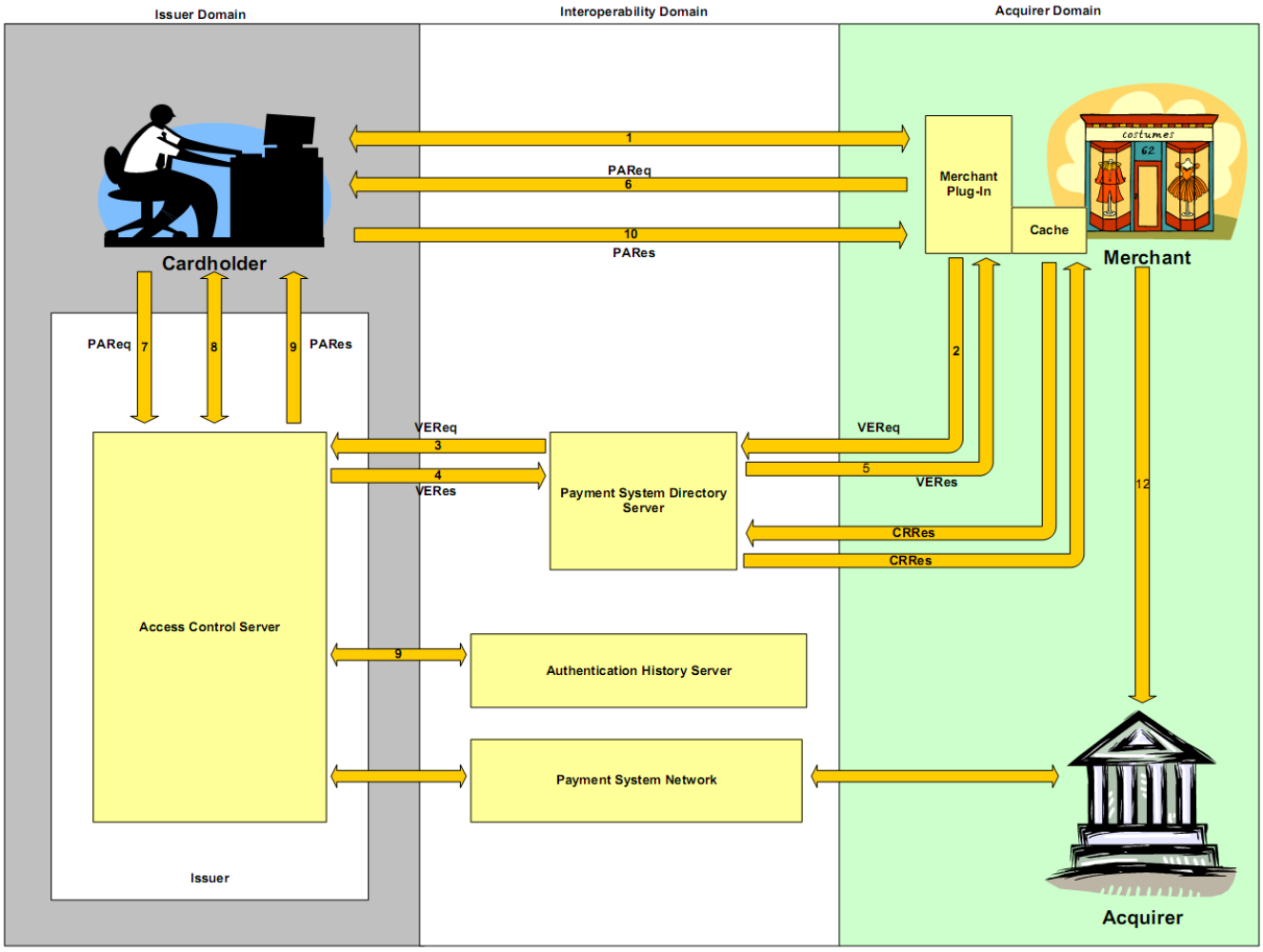

Рис. 2. Трехдоменная схема осуществления платежа в Интернете, с разбиением на этапы

1. Покупатель выбирает необходимые товары в электронном Интернет-магазине ТСП и формирует «корзину» заказа.
2. Дополнительный программный модуль Merchant Plug-In (MPI) генерирует запрос на проверку регистрации (VEReq) на сервер МПС для определения доступности аунтентификации данной конкретной карты.
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.

4. ACS-Сервер отвечает Серверу Каталога с ответом VERes, отмечая, доступна ли аутентификация для номера карты.
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.
6. Модуль MPI посылает запрос на аутентификацию плательщика (PAReq) для ACS-Сервера с помощью браузера покупателя, предоставляя данные, необходимые для попытки аутентификации ДЕРЖАТЕЛЯ КАРТЫ.
7. ACS-Сервер получает запрос PAReq.
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.

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.
10. Модуль MPI получает ответ PARes.
11. Модуль MPI подтверждает подпись ответа PARes (или производя подтверждение самостоятельно или передавая сообщение на отдельный Сервер подтверждения (Validation Server)).
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 случаи 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 Порядку на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет

ЗАЯВЛЕНИЕ НА ОПЕРАЦИЮ

_____
(наименование Клиента и сайта/Интернет-площадки)

☐ Расходная Операция[1] ☐ Частичная отмена[2] ☐ Полная отмена[2] ☐ Возврат[2]

Управляющему Филиала _____ АКБ Капиталбанк

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 Клиента:
Руководитель

_____ _____
подпись ФИО

Главный бухгалтер

_____ _____
подпись ФИО

М.П.

«____»_____ 201__г.

[1]Оформляется в случае отсутствия технической возможности самостоятельно выполнить операцию или в нестандартных случаях
[2]Может быть оформлено Клиентом 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, спроцессировать 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 Клиента:
Руководитель

_____ _____
подпись ФИО

Главный бухгалтер

_____ _____
подпись ФИО

М.П.«____» _____ 201__г.

Приложение № 4
к Порядку на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет

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 Порядку на предоставление услуг электронной коммерции по картам международных платежных систем через Интернет

Merchant application form.
Форма о деятельности организации.

Corporation details. Данные организации.	
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.	
Bank account information – Данные банковского счета	
Main Account Основной счет	
Bank name Банк	
Account number Номер счета	
Bank branch МФО	
Swift code Свифт	
Website details – Данные вэб сайта	
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	
Website content / Наименования продукта/товаров.	
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 police 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.	