

ПОРЯДОК, УСЛОВИЯ И ОТВЕТСТВЕННОСТЬ СТОРОН ПРИ ПОДКЛЮЧЕНИИ QR-API

1. Термины

QR-API – программные интерфейсы взаимодействия между системами Банка/партнёров Банка, применение которых позволяет Предприятию использовать функционал «Плати QR», а также предоставляет Предприятию возможность использования QR-кода для оплаты товаров/услуг.

Порядок – настоящий Порядок, условия и ответственность сторон при подключении QR-API.

Приложение Предприятия (Приложение) – любое программное обеспечение, имеющее техническую возможность вызова QR-API, которое Предприятие планирует подключить/подключило к QR-API.

Учётные сведения – создаваемая Предприятием или по его поручению совокупность данных и средств (в том числе, но не ограничиваясь: API-Ключ (access_token), идентификатор Приложения (Client_ID) и пароль Приложения (Client_Secret)), сведения о которых хранятся в компьютерной системе Банка, необходимых для распознавания (аутентификации) Предприятия/Приложения Предприятия и предоставления возможности информационно-технологического взаимодействия посредством QR-API.

TLS (Transport Layer Security) – криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет.

Иные термины и определения, используемые в настоящем документе и написанные с заглавной буквы, имеют те же значения, что и в Условиях проведения расчетов между ПАО Сбербанк и Предприятием по операциям с использованием банковских карт (эквайринг).

2. Порядок использования QR-API

2.1. QR-API (в т.ч. всё, что связано с организацией информационно-технологического взаимодействия посредством такого API) предоставляется Банком «как есть» без предоставления каких-либо гарантий. Предприятие осознает и соглашается с тем, что использует API на свой собственный риск и без каких-либо гарантий.

2.2. Банк не несет ответственности за понесенные Предприятием и/или третьими лицами убытки, причиненные в результате использования или невозможности использования QR-API или отдельных его частей/функций, в том числе из-за возможных ошибок или сбоев в работе API, вне зависимости от наличия у Банка сведений или предположений о возможности возникновения таких убытков.

2.3. Все права на QR-API и программное обеспечение, посредством которого обеспечивается работа API на стороне Банка, принадлежат Банку. Предприятию разрешается использовать API и сведения, передаваемые посредством QR-API, в границах прав и функциональных возможностей такого API и его описания, изложенного в настоящем Порядке.

2.4. В случае приостановления/прекращения доступа Предприятия/Приложения к QR-API (в т.ч. возможности начала использования QR-API) вследствие нарушения условий настоящего Порядка и/или по техническим причинам, Предприятие самостоятельно и в полном объеме несет ответственность перед третьими лицами, предъявляющими претензии в этой связи.

2.5. Предприятие самостоятельно и в полном объеме **несёт ответственность** перед Банком и третьими лицами за:

2.5.1. Использование (в т.ч. несанкционированное) и сохранность (в т.ч. неразглашение) своих Учетных сведений. Предприятие самостоятельно несет риск возможных неблагоприятных для него и (или) Банка последствий, связанных с утерей или разглашением предоставленных Учетных сведений.

2.5.2. Соблюдение требований законодательства Российской Федерации и законодательства местонахождения Предприятия при использовании QR-API. Если использование Предприятием какой-либо функциональности, предоставляемого API, может повлечь нарушение законодательства, Предприятие обязуется воздержаться от использования API в целом.

2.6. Предприятию запрещается:

2.6.1. Использовать QR-API для расширения функциональных возможностей сайтов/приложений, содержание которых нарушает или может повлечь нарушение российского законодательства или иного применимого законодательства, права и законные интересы третьих лиц.

2.6.2. Использовать любое программное обеспечение, устройства или иные средства, позволяющие получить Учетные сведения с нарушением порядка получения таких сведений, установленного Банком.

2.6.3. Вмешиваться в работу QR-API, совершать попытки влияния на функциональность и работоспособность API.

2.6.4. Злоупотреблять доступом к QR-API путем направления неограниченного числа вызовов API (в том числе, но не ограничиваясь: с целью нарушения работы автоматизированных систем Банка или API).

2.6.5. Осуществлять действия, в т.ч. с использованием QR-API, направленные на несанкционированный доступ к информационно-вычислительным и сетевым ресурсам Банка, а также на нарушение корректной работы оборудования и сетей, не принадлежащих Предприятию.

2.6.6. Осуществлять с использованием API действия, прямо или косвенно направленные на причинение убытков (прямых и косвенных) Банку.

2.7. Банк вправе самостоятельно квалифицировать действия Предприятия/Приложения на предмет нарушения положений настоящего Порядка и блокировать доступ к QR-API без предварительного предупреждения.

2.8. Все действия с использованием Учетных сведений Предприятия считаются совершенными таким Предприятием. Предприятие соглашается с тем, что несет полную ответственность за любые действия, совершенные с использованием его Учетных сведений, равно как и за последствия таких действий.

2.9. Банк вправе:

2.9.1. Вносить изменения в QR-API, а также в объем данных, передаваемых Предприятию/Приложению.

2.9.2. Осуществлять мониторинг всей деятельности по использованию API, а также собирать и анализировать статистику действий Предприятия/Приложения, осуществленных с помощью API.

2.9.3. Проводить технические работы в любой момент времени.

2.9.4. Блокировать доступ Предприятия/Приложения к QR-API без предварительного предупреждения.

2.10. В соответствии со ст. 431.2 ГК РФ Предприятие заверяет Банк в достоверности следующих сведений и обстоятельств, имеющих значение для Договора, а именно: лица, которым с помощью функциональных возможностей интернет-ресурсов или иным способом (в т.ч. с помощью Учетных сведений) предоставлены права/возможность совершать действия от имени Предприятия (в том числе, но не ограничиваясь: возможность создания Приложений, организации информационно-технологического взаимодействия с помощью API, вызова API), равно как и совершать иные действия, связанные с исполнением Договора, являются уполномоченными Предприятием лицами (имеют соответствующую доверенность) на совершение как указанных, так и иных действий, связанных с исполнением Договора.

Предприятие, в соответствии со ст. 431.2 ГК РФ, возмещает Банку все убытки, возникшие из-за недостоверности указанных в настоящем пункте гарантий и заверений Предприятия и предъявления в связи с этим к Банку претензий и/или требований о возмещении потерь и/или убытков, возникших вследствие неправомерного использования Учетных сведений Предприятия и совершения иных действий, связанных с исполнением Договора.

2.11. Предприятие признает все документы (в т.ч. электронные сообщения, заявки и прочие обращения), направленные (в т.ч. с помощью Учетных сведений) или полученные им посредством электронных каналов взаимодействия в рамках Договора (в т.ч. с помощью API), равно как и журналы учета действий Предприятия, формируемые автоматизированными средствами Банка, юридически значимыми для целей Договора.

2.12. Предприятие обязуется:

2.12.1. Предоставлять в Банк изменившиеся контактные сведения и прочую информацию о Предприятии (контактные телефоны, почтовый адрес, адрес местонахождения, URL-адрес сайта, виды деятельности), не позднее 7 (Семи) рабочих дней с даты их изменения.

2.12.2. При выявлении фактов или признаков нарушения безопасности использования QR-API и функциональных возможностей организации информационно-технологического взаимодействия немедленно приостановить использование API и оповестить об этом Банк любым способом, указанным в Договоре на проведение расчетов между ПАО Сбербанк и Предприятием по операциям с использованием банковских карт (эквайринг).

2.13. Предприятие соглашается с организацией информационно-технологического взаимодействия с помощью QR-API посредством сети Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, принимая на себя все риски, связанные с подключением его вычислительных средств к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет.

3. Требования к каналу информационно-технологического взаимодействия с помощью QR-API:

3.1. Тестовый доступ к API может получить любой зарегистрировавшийся на портале Пользователь.

3.2. Для подключения к промышленному API необходим выпуск клиентского сертификата для Приложения, созданного в личном кабинете на портале Сбербанк для разработчика: <https://developer.sberbank.ru/>. Срок действия сертификата один календарный год. Перевыпуск сертификата осуществляется в личном кабинете на портале.

3.3. Для обеспечения необходимого уровня защиты канала связи между Предприятием и Банком используется двустороннее TLS соединение. Шифрование передаваемых данных осуществляется посредством серверного сертификата шлюза API Сбербанка, клиентского сертификата и закрытого ключа, выпущенных для Приложения Предприятия. Закрытый ключ известен только Предприятию и никому не должен передаваться.