Консолидированные Процедуры безопасности TTS

Как установлено в Разделе «Сообщения» Общих условий ведения Счета и оказания Услуг (или других применимых условий обслуживания счетов) («Общие условия»), заключенными между Клиентом и Банком, ниже описываются процедуры безопасности («Процедуры»), используемые Департаментом по развитию банковских продуктов (Citi Treasury и Trade Solutions) в связи со следующими Услугами или каналами связи.

- CitiDirect BE® (в том числе Электронное управление банковским счетом (“eBAM”), TreasuryVision®, и WorldLink®)
- Интерактивный речевой ответ (“IVR”)
- Электронная почта/факс с Банком за исключением платежных инструкций на бумажном носителе (MIFT)
- CitiConnect®
- Другие местные электронные каналы связи

Доступность Услуг или каналов связи будет отличаться в зависимости от условий местных рынков. Настоящие Процедуры могут время от времени пересматриваться и такие изменения могут время от времени доводиться до Клиента с помощью электронных средств связи или иным образом. Использование Клиентом любой из вышеперечисленных Услуг или каналов связи после того, как будет проинформирован о пересмотре и обновлении Процедур (что может включать, помимо прочего, публикацию обновленных процедур на CitiDirect BE, в отношении услуг или канала связи), будет считаться принятием таких пересмотренных процедур. Эти Процедуры должны читаться совместно с Общими условиями, так как время от времени в Общие условия могут вноситься изменения. Термины, указанные с заглавной буквы, определение которых не приводится в настоящем документе, должны иметь значения, присвоенные им в Общих условиях.

A. Функции и обязанности Администратора*

Для приложений, доступных в CitiDirect BE, Банку необходимо два человека для ввода и авторизации инструкций; поэтому требуется, как минимум, два Администратора. Любые два Администратора, действуя согласованно, могут давать инструкции и / или подтверждения через каналы связи в отношении любой функции Администратора или для обеспечения нашего взаимодействия через Интернет. Любые такие Сообщения, если они авторизованы двумя Администратора, будут приниматься и исполняться Банком. Банк рекомендует назначить не менее трех Администраторов для обеспечения взаимозаменяемости. Клиент назначает своих Администраторов, используя Заявление на подключение к Каналам. Администратор Клиента также может действовать в качестве Администратора для Счета(ов) компаний - третьих лиц (например, аффилированного предприятия Клиента) и осуществлять все связанные с этим права (включая назначение пользователей для Счета(-ов) такого предприятия-третьего лица), без какого-либо дополнительного назначения, если такая компания -третье лицо подпишет форму Разрешения на предоставление универсального доступа (или любую другую форму

авторизации доступа, приемлемую для Банка), предоставляя Клиенту доступ к его Счету(-ам). Это применяется только в отношении Счета(-ов), на которые распространяется в соответствующее разрешение.

* Функции и обязанности Администратора могут быть запрещены на определенном местном рынке. Для получения дополнительной информации, свяжитесь с представителем отдела операционного обслуживания клиентов.

Функции Администратора включают, помимо прочего:

1. Предоставление и текущая поддержка доступа и прав пользователей (включая самих Администраторов), в том числе следующие функции как:
    (a) создание, удаление или изменение Профилей Пользователя (в том числе Профилей Администраторов) и наделение полномочиями (обратите внимание, что имя пользователя должно совпадать с удостоверяющими документами)
    (b) создание профилей доступа, которые определяют функции и данные, доступные различным пользователям, а также
    (c) подключение и отключение учетных данных входа.
2. Создание и изменение записей в поддерживаемых Клиентами библиотеках данных (таких как шаблоны платежей и библиотека бенефициаров), а также предоставление разрешений другим пользователям делать то же самое.
3. Изменение последовательности авторизации (одобрения) платежей.
4. Присвоение динамического идентификатора или паролей доступа к системе для пользователей Клиента.
5. Уведомить Банк, если есть любые основания подозревать, что безопасность была нарушена.

Администраторы вправе назначать (устанавливать) лимиты операций для пользователей тех продуктов Банка, к которым у Клиента есть доступ. Банк не контролирует и не одобряет такие лимиты; Клиент обязан самостоятельно отслеживать такие лимиты в целях обеспечения соблюдения внутренних политик и требований Клиента, включая, помимо прочего, те, которые установлены Советом директоров Клиента или уполномоченными органами Клиента.

В частности, для **Приложения eBAM** необходимо назначить следующих лиц:

Первоначальная настройка Услуги eBAM требует назначения трех Сотрудников безопасности и одного Корпоративного секретаря. Два отдельных Старших администратора действуют согласованно как создатель / проверяющий для настройки и определения пользовательских прав на выполнение функций/доступа к данным, а также определения последовательности действий процесса. Банк не контролирует/не проверяет такие настройки; последовательность действий и деятельность пользователя контролируется Клиентом в целях обеспечения соблюдения внутренних политик Клиента (а также владельцев Счета), а также его требований, уровней авторизации и согласования, в том числе, помимо прочего, тех, которые были установлены Советом директоров Клиента (Владельца счетов) или эквивалентным компетентным органом.

Для Услуги eBAM потребуется назначить следующих лиц:

1. **Сотрудник безопасности:** выполняет функции, указанные в пункте (1) a-c выше, в рамках функций Администратора.
2. **Корпоративный секретарь:** обеспечивает Последовательность Авторизаций, назначение Пользователей в качестве Авторизаторов, и их назначение в рамках Последовательности Одобрений соответствующее внутренним политикам, уровню авторизации и одобрения Клиента (а также владельца Счета), в том числе, помимо прочего, тем, которые были установлены Советом директоров Клиента (Владельца Счета) или равнозначным компетентным органом.
3. **Авторизатор:** имеет широкие права и полномочия для инициирования и авторизации действий в рамках рабочего процесса.
4. **Инициаторы запросов:** это лица, уполномоченные выполнять действия по администрированию, такие как оформление заявок и заявка по созданию счета и управление перечнем подписантов в системе eBAM.

Сотрудники безопасности, Корпоративный секретарь и Авторизаторы отвечают за:

a) Определение и администрирование установки иерархии и управления сайтом / потоком, как то, установление Последовательности авторизации, определение Пользователей и уровней одобрения.
b) Создание дополнительных ролей Старших администраторов и назначение Пользователей (которые не обязательно должны быть работниками Клиента).
c) Уведомление Банка, если есть основания подозревать, что безопасность или конфиденциальность любых прав пользователя (включая Старших администраторов) были нарушены или скомпрометированы.
d) По мере необходимости, заполнение, внесение изменений, одобрение и/или дополнение таких форм, заполняемых Клиентом, которые могут время от времени обоснованно запрашиваться Банком в связи с предоставлением Клиенту продуктов и / или услуг.

B. Способы аутентификации

Процедуры включают в себя определенные защищенные способы аутентификации («Способы аутентификации»), которые используются для достоверной идентификации и проверки полномочий Клиента и/или любого из его пользователей, как правило, с помощью таких механизмов, как: пара уникального идентификатора пользователя / пароль, цифровые сертификаты и токен безопасности (применяемые с помощью аппаратного или программного обеспечения), которые генерируют динамический пароль, используемый для получения доступа к услугам или каналам связи каждый раз, когда Клиент или пользователь регистрируется или аутентифицируется сам. Следует обратить внимание на то, что доступность Способов аутентификации, описанных ниже, зависит от условий местных рынков.

Администраторы и все пользователи, которые хотят (а) инициировать или одобрить операции (и чей Профиль пользователя позволяет им это делать) и/или (б) получить доступ к системам в соответствии с его правами, и обязаны использовать доступные Способы аутентификации (которые могут пересматриваться время от времени, как описано выше).

Следующие Способы аутентификации доступны для получения доступа к вышеупомянутым услугам или каналам связи в сочетании с идентификатором пользователя (User ID):

Способы аутентификации	**Описание**
Токен: механизм вызов-ответ	Либо (i) мобильный программный токен (Mobile Soft Token) (на основе мобильного приложения) (например, MobilePASS), либо (ii) токен с аппаратной реализацией функций шифрования (например, SafeWord Card, Vasco), который в каждом случае используется для генерирования динамического пароля после аутентификации с помощью 4-значного пин-кода. При доступе к CitiDirect BE система генерирует вызов, а ответный код-пароль генерируется с помощью применимого токена и вводится в систему.
Токен: одноразовый пароль	Либо (i) мобильный программный токен (Mobile Soft Token) (на основе мобильного приложения) (например, MobilePASS), либо (ii) токен с аппаратной реализацией функций шифрования (например, SafeWord Card, Vasco), который в каждом случае используется для генерирования динамического пароля после аутентификации с помощью 4-значного пин-кода. Этот динамический пароль вводится в систему для получения доступа.
Одноразовый код по SMS	Динамический пароль отправляется пользователю через SMS, после чего пользователь вводит динамический пароль и защищенный пароль для получения доступа к системе
Голосовой одноразовый код	Динамический пароль предоставляется пользователю с помощью автоматического голосового вызова, после чего пользователь вводит динамический пароль и защищенный пароль для получения доступа к системе
Многофакторная аутентификация	Динамический пароль генерируется с помощью токена SafeWord Card или MobilePASS, после чего такой динамический пароль вводится вместе с защищенным паролем для получения доступа к системе.
Цифровые сертификаты	Цифровой сертификат, выданный уполномоченным органом сертификации, который используется для аутентификации. Цифровые сертификаты используют механизм хранения ключа и соответствующий PIN-код и могут быть выпущены IdenTrust, SWIFT (3SKey) или другими согласованными провайдерами.
Безопасный пароль	Пользователь вводит свой безопасный пароль для получения доступа к системе. Безопасный пароль обычно ограничивает возможности пользователя в системе, так что информация может быть просмотрена, но нет возможности провести операцию.
Интерактивный голосовой ответ (“IVR”) и электронная почта	Пользователям, обращающимся в банк, будет предложено ввести PIN-код или предоставить другую информацию для подтверждения авторизированного доступа по телефону или по электронной почте
Факс	Полученный Банком документ, за исключением заявок MIFT, будет проверен на подлинность подписи на основе информации, которая содержится в решении Совета директоров Клиента.
MTLS	Протокол Mandatory Transport Layer Security (MTLS) (Протокол защиты транспортного уровня) создает безопасное частное соединение по электронной почте между банком и внешней стороной. Электронное письмо, отправленное с

	использованием этого канала, отправляется через Интернет через зашифрованный канал TLS, созданный соединением.
Защищенный паролем файл PDF	Зашифрованные электронные письма доставляются в обычный почтовый ящик в виде документа в формате PDF, который открывается с помощью личного пароля, при этом и само сообщение, и все прикрепленные файлы зашифровываются. Личный пароль можно настроить после получения первого сообщения по защищенной электронной почте.

Более подробная информация о любом из этих Способов аутентификации представлена на странице Login Help на CitiDirect BE®: (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

Для CitiConnect®

- Если Клиент желает использовать общедоступное интернет соединение для подключения к Citi, включая протоколы HTTPS, защищенные протоколы FTP и FTPS, Банк и Клиент обменяются сертификатами безопасности, чтобы гарантировать, что и канал связи, и высылаемые сообщения полностью зашифрованы и защищены. Банк принимает только сообщения, исходящие из защищенного шлюза связи Клиента, с использованием полученных в результате обмена сертификатов безопасности, и наоборот, и Банк будет передавать сообщения только в шлюз связи Клиента с помощью полученного сертификата безопасности.
- Если Клиент решит использовать CitiConnect через SWIFT, то для любых платежных поручений и указаний, посредством SWIFT, включая изменение или отмену таких указаний, для проверки подлинности того, что платежное поручение или указание исходит от Клиента и авторизовано Клиентом, должны применяться Процедуры, предусмотренные в Договоре на обслуживание SWIFT (как это термин определен SWIFT, с учетом вносимых в определение время от времени поправок и дополнений), которая включает в себя, помимо прочего, Общие положения и описание услуги FIN или как предусмотрено в любых других условиях, которые могут быть установлены SWIFT. Банк не несет ответственности за какие-либо ошибки или задержки в системе SWIFT. Сообщения Банку должны направляться в таком формате и в таком виде, который требуется и указан SWIFT.
- При использовании VPN Клиент и Банк указывают один IP-адрес, с которого будут отправляться и/или получаться Сообщения между Клиентом и Банком. Банк будет принимать только Сообщения, исходящие из указанного IP-адреса Клиента, и наоборот, и Банк будет направлять сообщения только на указанный IP-адрес Клиента.
- Клиент и Банк могут также использовать Способы аутентификации аппаратного модуля защиты данных в дополнение к аутентификации VPN. Для этого необходимо, чтобы и Банк, и Клиент установили устройство на серверах, предназначенное для передачи Сообщений между Банком и Клиентом.

Банк требует:

- Принятие Клиентом обеспечения мер безопасности в отношении Способов аутентификации, включая параметры доступа к системе и/или сертификатов безопасности,

связанных со Способами аутентификации (совместно именуемые «Данные авторизации для входа в систему») и обеспечение того, чтобы доступ и Данные авторизации для входа в систему имелись только у тех лиц, которые были уполномочены Клиентом. Способы аутентификации и связанные с ними Данные авторизации для входа в систему - это методы, с помощью которых Банк проверяет принадлежность Сообщений, направляемых Клиентом Банку.

- Клиент должен принять все разумные меры для защиты Данных авторизации для входа в систему. Соответственно, Банк настоятельно рекомендует Клиенту не передавать Данные авторизации для входа в систему третьим лицам.

В некоторых юрисдикциях может требоваться, чтобы лица (и их соответствующие данные авторизации для входа в систему) были идентифицированы на соответствие применимым требованиям законодательства о противодействии легализации денег, полученных преступным путём, прежде чем им будет предоставлен доступ для выполнения определенных функций.

Банк понимает, что Клиент вправе в некоторых случаях пожелать передать Данные авторизации Клиента для входа в систему сторонним лицам или провайдеру услуг (в том числе, помимо прочего, поставщику услуг по начислению заработной платы, который является третьим лицом), указанным Клиентом для предоставления доступа к данным авторизации Клиента (такие третьи лица или провайдеры услуг именуются в дальнейшем «Уполномоченные третьи лица») в целях получения доступа и использования любого из банковских электронных каналов от имени Клиента. В случае, когда Клиент решит предоставить свои Данные авторизации для входа в систему Уполномоченным третьим лицам, Банк настоятельно рекомендует, чтобы Клиент самостоятельно предпринял и обеспечил, чтобы любая Уполномоченная третья сторона приняла все разумные меры для защиты Данных авторизации от их раскрытия неавторизованному персоналу третьей стороны. Банк уполномочивается действовать после получения Сообщения от Уполномоченной третьей стороны от имени Клиента в соответствии с данными Процедурами.

C. Целостность данных и Защищенная связь

- Клиент будет передавать данные и иным образом обмениваться сообщениями с Банком, используя Интернет, электронную почту и/или факс, и эти средства связи не обязательно являются безопасными способами связи и передачи данных. Банк использует передовые, принятые в отрасли, методы шифрования (определяемых самостоятельно Банком), которые помогают обеспечить конфиденциальность информации и невозможность изменения данных во время их передачи.
- Если Клиент подозревает или ему становится известно о техническом сбое или несанкционированном доступе, или ненадлежащем использовании услуг Банка, каналов подключения или Способов аутентификации любым лицом (независимо от того, является ли оно уполномоченным лицом или нет), Клиент должен незамедлительно уведомить Банк об этом. В случае, если уполномоченное лицо Клиента получило ненадлежащим образом доступ или воспользовалось услугами или каналами связи, то Клиент должен

незамедлительно принять меры для прекращения доступа такого уполномоченного лица к услугам и каналам связи Банка и их использованию.

- Если Клиент использует программное обеспечение для форматирования файлов и шифрования (независимо от того, предоставлено ли оно Банком или третьим лицом) для поддержки форматирования и распознавания данных и инструкций Клиента и действует в отношении сообщений с Citi, то Клиент будет использовать такое программное обеспечение исключительно для тех целей, для которых оно было установлено.
- Клиент соглашается с тем, что Банк может приостановить доступ Пользователей к Услугам, которые требуют использования Данных авторизации для получения доступа к системе (i) в случае подозрения в несанкционированном или мошенническом использовании Данных авторизации и/или (ii) для того, чтобы защитить Услуги и / или Данные авторизации.