Техническое задание на проведение тендера по выбору поставщика для внедрение мобильного приложения для работы с инвестициями.

Срок предоставления ТКП	**14.01.2022**
Адрес направления ТКП	kuklin@sngb.ru, a.loboda@sngb.ru
Контакты	**+7 (3462) 39-88-88 доб. 2032**

1.

I. Требования Банка к мобильному приложению для работы с инвестициями.

1. **Цели проекта:**
   a) **Увеличение клиентской базы по брокерскому обслуживанию на 5% в течение года после внедрения отдельного мобильного приложения для инвестиций**
   b) **Увеличение количества активных клиентов (одна и более сделок в месяц) на 50 %.**
2. **Задачи проекта:**
   a) **Предоставить для клиентов Банка новую интерфейсную форму для управления операциями, которые в настоящее время выполняются в интерфейсе QUIK**
   b) **Предоставить для клиентов Банка конкурентную платформу по инвестициям.**

3. **Функционал по инвестициям в отдельном приложении:**
   a) **Поддержка возможности направления PUSH уведомлений (поддержка SMS в случае недоставки PUSH)**
   b) **Встраивание / поддержка чата с оператором**
   c) **Поддержка входа по Touch-id / Face-id (автоматически всплывает при открытии), поддержка входа по PIN коду**
   d) **Вход в МП по мобильному телефону**
   e) **Отдельный раздел «Избранные бумаги / инструменты»**
   f) **Отдельный раздел «Уведомления» (аналогично СНГБ Онлайн)**
   g) **Отображение лимитов по деньгам и по бумагам**
   h) **Операции пополнения счета выполняются в СНГБ Онлайн / либо прикручиваем e-comm для списания с карты и пополнения счета (30601) в Банке.**
   i) **Отдельный раздел «Профиль» (изменить пароль, настроить вход по отпечатку, по PIN, настройка SMS PUSH уведомлений)**
   j) **Ключевой функционал по инвестициям**
   k) **Поддержка «Stories»**

№№	Действующий функционал в «СНГБ Онлайн»	Планируемый к внедрению функционал в МП «Инвестиции»	Pocket QUIK
1.	Подача поручений на покупку/продажу ЦБ по текущей цене	Стакан котировок	Стакан котировок
2.	Пополнение/вывод средств	Покупка/продажа ЦБ по лимитированным ценам	Графики с основами теханализа
3.	Подключение QUIK/iQUIK	Графики котировок	Стоп-заявки
4.	Заказ отчетов по сделкам/договоров/выписок	Признание квал. инвестором	Настраиваемые показатели таблиц котировок
5.		Проведение онлайн тестирования не квал. инвесторов	Настраиваемые показатели портфеля клиента
6.		Формирование инвестиционного профиля клиента (анкета с вопросами)	Возможность настройки нескольких таблиц котировок
7.		Графики выплат купонов, история выплат дивидендов.	Объединение нескольких портфелей клиента.
8.		Аналитика по портфелю клиента (стоимость / доходность портфеля за период, по отраслям, по валюте)	
9.		Аналитические материалы / консенсус прогнозы по эмитентам ЦБ	
10.		Формирование и отправка формы W-8BEN	
11.		Маржинальная торговля	
12.		Формирование отчетов (документ, который можно сохранить на устройстве). Банк выгрузит из АБС историю сделок / операций	
13.		Доступ ко всем режимам торгов, доступных в QUIK (валютные, фондовые, металлы, облигации и др.)	
14.		История операций	
15.		Новостная лента (получение контента	

		через API поставщика новостей: Reuters / InterFax)	
16.		Профиль, настройки клиента	
17.		Стоп-заявки	

4. **Публикация в сторах:**
    1. **Apple Pay (поддержка версии iOS не старше 10)**
    2. **Play Market (поддержка версии Android не старше 7)**
    3. **App Gallery**
5. **Ограничения:**
    a) **Приложение является дополнительным к СНГБ Онлайн**
    b) **В качестве серверной части используется QUIK**
    c) **Бэкенд в виде Сигнатор/FM и АБС**
    d) **Функционал, реализованный в «СНГБ Онлайн» по инвестициям не мигрирует**
    e) **Система предназначена только для физических лиц**
    f) **Web- версии системы не предполагается**
6. **Требования к дизайну**
    a) **Должен быть отдельный блок для рекламы, акций, новостей, рекомендаций, корпоративные события и прочее**
    b) **Свой дизайн для планшетной версии**
    c) **Поддержка новой концепции дизайна «СНГБ Онлайн»**
    d) **Поддержка темной темы для премиального сегмента**
    e) **Сервис рассылки ПУШ уведомлений с внутренними и внешними диплинками**

7. **Документирование:**
    a) **Техническое задание на разработку (в том числе требования по ИБ)**
    b) **Спецификация программных требований**
    c) **Руководство администратора**
    d) **Руководство пользователя**
    e) **Сценарии тестирования**
8. **Возможные роли**
    a) **Пользователь**
    b) **Администратор**
    c) **Администратор контента**

9. **Требования к безопасности:**

II. Требования к информационной безопасности

Безопасность соединения:

1. Взаимодействие между Мобильным клиентом и сервером ДБО должно происходить в защищенном режиме на базе HTTPS via TLS не ниже версии 1.2.
    a. Длина ключа по документации:
        i. Симметричные: от 256
        ii. Ассиметричные: от 4096
    b. Используется стандартный для платформы криптопровайдер или механизмы, аналогичные криптопровайдеру.
2. Заказчик на этапе разработки/внедрения должен предоставить необходимый сертификат для реализации данных требований (например, SSL Trusted Certificate).
    a. Сертификат автоматически не обновляется. Для обновления требуется перевыпустить приложения.
    b. Список отозванных сертификатов не поддерживается.

Аутентификация и авторизация:

1. Обмен аутентификационными / авторизационными данными между компонентами разрабатываемой Системы, а также между разрабатываемой Системой и сервисами Банка должен проходить в защищенном режиме на базе HTTPS.
2. Минимальные версии протоколов, которые должна поддерживать система:
    a. TLS1.2
3. Шифры согласуются на этапе реализации. Подбираются исходя из требований минимально поддерживаемых версий платформ и требований банка.

Контроль целостности приложений:

1. Публикуемые мобильные приложения подписываются сертификатами, действительными для данной конкретной платформы.
2. Контроль целостности мобильных приложений осуществляется стандартными средствами платформы.

3. В случае нарушения целостности либо не подтверждения сертификата, сама платформа не позволяет установить либо запустить приложение.

Требования к безопасности данных:

1. Мобильный банк должен выполнять очистку временных данных каждый раз при закрытии приложения/выходе пользователя из системы.
2. Реализация должна исходить из принципа минимизации времени хранения конфиденциальных данных при работе приложения.
3. Конфиденциальные данные запрещено хранить:
    a. на SD-карте,
    b. в системном буфере обмена данными между приложениями,
    c. каких-либо журналах/логах,
    d. без явной необходимости в памяти устройства в открытом виде.
4. Должна быть предусмотрена защита от ошибок переполнения буфера, в том числе:
    a. Применение техник защитного программирования,
    b. Явная проверка всех входных данных на допустимый максимум,
    c. Мониторинг обнаруженных проблем и обновлений безопасности в системном ПО и своевременное обновление при обнаружении проблем.

Программный код:

1. Программный код не должен содержать:
    a. Программных закладок,
    b. Скрытого функционала,
    c. Иных недекларируемых возможностей, в том числе средств тестирования.
2. Мобильное приложение не должно содержать уязвимостей из списков OWASP GUIDE и SANS CWE Top 25.

Кэширование:

1. Компоненты Системы не должны кэшировать:
    a. пароль,
    b. аутентификационные данные пользователей,
    c. номера карт,
    d. прочие конфиденциальные данные.
2. Полный набор данных, которые разрешено кэшировать на стороне клиентского рабочего места определяется на этапе разработки.

Сессионность:

1. Должны быть предусмотрены следующие таймауты сессии Пользователя:
    a. На клиентской части;
    b. На серверной части.

Аудит:

1. Должны быть предусмотрены средства аудита и протоколирование данных для операций, выполняемых в Системе.
2. События аудита:
    a. регистрируются в базе данных,
    b. могут быть использованы позже как для анализа действий отдельного Пользователя, так и использования Системы в целом.
3. Каждая запись в журнале аудита состоит из:
    a. Системной информации – согласно **Ошибка! Источник ссылки не найден.**;
    b. Бизнес информации – данные, характеризующие действие Пользователя: Действие, Успешность действия, Тело запроса клиента (http или xml), Тело ответа на запрос клиента.
4. Полный перечень действий для протоколирования уточняется на этапе разработки и приводится в документе «Спецификация требований».
    a. Отдельные данные об устройстве/ПО Пользователя могут быть не определены по техническим причинам (отсутствуют, платформа устройства не передает данные, и т.д.).

Поддержка требований Положения Банка России №382-П

В рамках проекта осуществляется поддержка только тех требований Положения №382-П, которые перечислены в Табл.«Поддержка требований 382-П»

Табл. Поддержка требований 382-П

	Требование	**Ответственная система**	**Описание реализации**
1.	Регистрация предоставления прав (всех) доступа к ПО	Аудит	Реализуется в рамках подсистемы «Аудит» (см. раздел 0)
2.	Уведомления клиентам о необходимости обновления приложений	Операционная система	Не реализуется в явном виде в системе ДБО. Используются следующие механизмы: 1. Встроенный в операционную систему механизм обновлений (на устройстве пользователя) 2. Самостоятельно проводимая Банком рассылка уведомлений клиентам.
3.	Возможность получения Банком информации о версии ПО, которую использует клиент	Аудит	Банк может получить эти данные: 1. Через модуль Аудит, 2. Путем личного контакта с клиентом (информация о версии должна отображаться внутри приложения «Мобильный банк»)
4.	**Регистрация действий при работе с ПО, используемом для осуществления переводов денежных средств**	Аудит	Реализуется в рамках подсистемы «Аудит» (см. раздел 0).
4.1.	- дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента;	Аудит	Реализуется в рамках подсистемы «Аудит» (см. раздел 0).
4.2.	- набор символов, присвоенный клиенту и позволяющий идентифицировать его в автоматизированной системе,	Аудит	Реализуется в рамках подсистемы «Аудит» (см. раздел 0).

	программном обеспечении;		
4.3.	- код, соответствующий выполняемому действию;	Аудит	Реализуется в рамках подсистемы «Аудит» (см. раздел 0).
4.4.	идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств	Аудит	Реализуется в рамках подсистемы «Аудит» (см. раздел 0).
5.	**Параметры операций** Банк устанавливает:	-	-
5.1.	- максимальную сумму перевода денежных средств с использованием системы Интернет-банкинга за одну операцию и (или) за определенный период времени (например, один день, один месяц);	Система Банка	Указанные параметры операций должны храниться и проверяться в Системах Банка. Система ДБО реализует: - Интерфейс пользователя для изменения настроек лимитов, - отображение сообщений, если система Банка сообщает, что пользователю запрещено выполнение операции.
5.2.	- перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга;	Система Банка	Указанные параметры операций должны устанавливаться и проверяться в Системах Банка. Система ДБО реализует отображение сообщений, если система Банка сообщает, что пользователю запрещено выполнение операции.
5.3.	- перечень устройств, с использованием которых может осуществляться доступ к системе Интернет-банкинга с целью осуществления переводов денежных средств, на основе идентификаторов указанных устройств;	Система Банка	Указанные параметры операций должны устанавливаться и проверяться в Системах Банка. Система ДБО реализует отображение сообщений, если система Банка сообщает, что пользователю запрещено выполнение операции.

5.4.	- перечень услуг, предоставляемых с использованием системы Интернет-банкинга;	Система Банка	Указанные параметры операций должны устанавливаться и проверяться в Системах Банка. Система ДБО реализует отображение сообщений, если система Банка сообщает, что пользователю запрещено выполнение операции.
5.5.	временной период, в который могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга.	Система Банка	Указанные параметры операций должны устанавливаться и проверяться в Системах Банка. Система ДБО реализует отображение сообщений, если система Банка сообщает, что пользователю запрещено выполнение операции.
6.	**Блокировка доступа**	-	-
6.1.	возможность блокирования учетной записи клиента	Система Банка	Система ДБО предоставляет возможность выполнить блокирование учетной записи из Системы Банка.
6.2.	возможность оперативной блокировки доступа на основании обращения клиента (с прекращением сессии работы с приложением)	Система Банка	Система ДБО предоставляет возможность выполнить блокирование учетной записи из Системы Банка.
7.	Запрет на хранение информации в мобильном устройстве по окончании сеанса использования системы мобильного банкинга	Мобильный банк	Описано в разделе 0

Поддержка разных версий мобильного приложения

1. Для обеспечения поэтапного перехода (обновления) Клиентов на приложения с поддержкой новой версии протокола используется несколько параллельно работающих версий серверной части Системы с разными версиями протокола.
2. При обращении клиентского приложения на сервер Системы ДБО определяется используемая им версия протокола.
    a. Если такая версия поддерживается одной из параллельно работающих серверных версий – запрос перенаправляется на данную версию.

b. Если нет – запрос отклоняется, Клиент получает сообщение о том, что не может работать с Системой ДБО и должен обновить свое приложение.

Требования к надежности и отказоустойчивости

1. Надежность должна достигаться за счёт:
   a. Проведения профилактических мероприятий по поддержанию технических и программных средств в работоспособном состоянии. Описание профилактических мероприятий будет указано в документе «Установка и администрирование.doc».
   b. Администрирования, мониторинга и периодической оптимизации баз данных и файловых каталогов;
   c. Обеспечения стабильного и бесперебойного электропитания технических средств с использованием средств резервного электропитания и энергоснабжения;
   d. Резервирования необходимых технических средств;
   e. Резервирования каналов связи;
   f. Использования специальных программных средств, в том числе Систем управления базами данных, обеспечивающих надежную обработку и хранение информации, проведение резервирования и восстановления информации.
2. Мероприятия, обеспечивающие надёжность и отказоустойчивость, должны проводиться Заказчиком.
3. Исправление функциональных ошибок должно проводиться Исполнителем в рамках договора на поддержку.

a) **Подтверждение операций кодом OTP**
b) **Блокирование / разблокирование пользователей**
c) **Требования к учетным записям**
d) **Безопасность сети и соединения**
e) **Аутентификация и авторизация**
f) **Программный код**
g) **Кэширование**
h) **Требования к парольной защите**
i) **Сессионность**
j) **Аудит**

k) **Требования к контролю целостности**
l) **Дополнительные требования**
m) **ОУД – 4 (если контрагент не передает исходный код, то должен предоставить подтверждение соответствия)**

a. **Прочие требования:**
   a) **Исходный код (исключительные права) после внедрения передается Банку**
   b) **Банку передаются все инструменты для самостоятельной сборки приложений**
   c) **Предоставить кликабельный прототип дизайна**
   d) **Поддержка возможности авторизации для неклиента Банка (регистрация новых клиентов по методу упрощенной идентификации)**
   e) **Поддержка цифрового профиля Госуслуг при регистрации**