Правила информационного взаимодействия между Банком и Предприятием

1. Вход по Сбер ID

Требования к предоставлению сервиса
а) Для работы с сервисом по получению расширенного набора данных (в частности, e-mail) с использованием PKCE[1] и универсальных ссылок.
(English version)
б) Для работы с сервисом без расширенного набора данных (в частности, без e-mail), PKCE и универсальных ссылок.

Требования к взаимодействию с Банком в зависимости от категории запрошенных данных
1. Для данных первой категории: ФИО, телефон.
Требуется установка сертификатов безопасности и настройка серверного ПО в соответствии с правилами Загрузки сертификата для одностороннего TLS соединения
Прим.: для компаний группы Сбера не допускается использование одностороннего TLS соединения.
2. Для данных второй категории: данные первой категории (см. выше) + любые дополнительные данные.
Допускается два варианта взаимодействия:

1. Требуется установка сертификатов безопасности и настройка серверного ПО в соответствии с правилами Загрузки сертификата для двустороннего TLS соединения.
2. Настройка соединения с использованием ФПСУ в соответствии с правилами Настройки соединения с использованием канала ФПСУ-IP.

Важно! В случае, если Предприятием выбран некорректный способ подключения, сервис не будет предоставлен.

На усмотрение Предприятия может быть выбран один из следующих способов взаимодействия с Банком:
1. Для использования сервиса с односторонним TLS соединением необходимо провести настройки в соответствии с Инструкцией.
2. Для использования сервиса с двусторонним TLS соединением необходимо провести настройки в соответствии с Инструкцией.
3. Для использования сервиса по каналу ФПСУ со стороны Предприятия необходимо загрузить серверный сертификат шлюза согласно Инструкции.

[1] PKCE (Proof Key for Code Exchange) предоставляет дополнительную защиту от использования токена аутентификации (AuthCode) в случае его перехвата по незащищенному каналу.