**Требования к безопасности**

Связь с Единой биометрической системой - через защищенные каналы связи на основе криптографического шифрования.

Мы не храним у себя фотографии людей, сохраняем историю запроса доступа и результаты запросов.

Партнерская система передает данные в SmartHome в зашифрованном виде по TLS 1.3.  
Сами данные, хранящиеся в SmartHome, также хранятся в зашифрованном виде.  
  
Доступ к данным имеют только те, кому они действительно нужны для работы.

Протокол обмена аутентификационными и авторизационными данными между SmartHome и Партнером - Security Assertion Markup Language.

**Как будет организовано взаимодействие между системами предприятия и внешней платформой?**

* Партнерская система передает в SmartHome номер устройства (домофона или шлагбаума), номер объекта недвижимости и аутентификационную информацию (фото человека, номера машины, перс. данные).  
  Также она, после получения команды от SmartHome, выполняет открытие или закрытие.
* Наша SmartHome получает от Партнера данные, по ним находит в Группе сервисов ЖКХ Собственника недвижимости.  
  Далее, если получено фото человека, SmartHome отправляет его в Единую биометрическую систему и в ответ получает перс. данные, которые сверяет у себя.  
  После сверки данных принимается решение предоставить доступ или отказать.  
  SmartHome собирает биометрию и регистрирует ее в ЕБС.  
  SmartHome по запросу Собственника в мобильном приложении отправляет команды на открытие / закрытие дверей и шлагбаума.