

# 5. 1С №00-00-XXXXXX. KeyCloak -> DWH

In Progress

## Бизнес требования для интеграции

1.1 Бизнес-заказчик: XXX.

Бизнес-цель интеграции: собирать данные о посещении пользователями ИС ФСК находящихся в DMZ и внешней сети и передавать их для дальнейшей аналитики.

Способ интеграции: забираем JSON данные через XXX протокол, XXX порт. При помощи валидации забираем только нужные данные. Фильтровать JSON на стороне KeyCloak не представляется возможным из-за отсутствия особенных компетенций и доработки коробочного решения написанного на Red Hat.

Как планируется забирать данные:

- логиниться через XXX в KeyCloak, которая будет отдавать XXX при условии, что согласуют паспорт интеграции;
- забирать только поля перечисленные в свойстве **XXX** из приложенной ниже JSON Schema;
- в забираемых полях фильтроваться по допустимым значениям через **регулярные выражения**;
- в случае если приходят нерелевантные значения данные **не пропускаются**;

1.2 Описание данных в формате JSON Schema

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "https://wiki.fsk.ru/pages/XXX",
  "title": "Сбор данных с Keycloak по посещаемости сервисов ГК ФСК находящихся в DMZ и внешней сети",
  "description": "Забираем массив объектов содержащих данные о сессии пользователя в сервисе",
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "XXX": {
        "type": "integer",
        "description": "Временная метка события в формате Unix (миллисекунды с эпохи)",
        "example": XXX
      },
      "XXX": {
        "type": "string",
        "description": "Тип события (в данном случае всегда XXX). Регулярка проверяет допустимые значения: XXX",
        "example": "XXX",
        "pattern": "^[a-zA      "
      },
      "XXX": {
        "type": "string",
        "description": "Идентификатор XXX, в котором произошло событие XXX",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
        "description": "Идентификатор XXX, через который XXX XXX",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
```

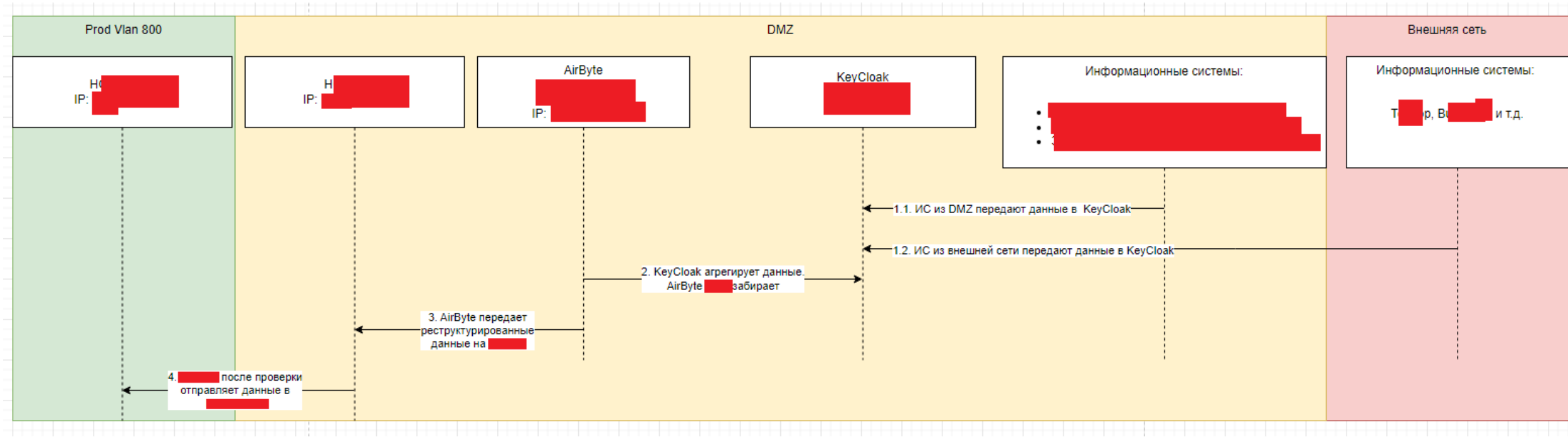
```
    "description": "Идентификатор XXX, который XXX XXX. Регулярка проверяет допустимые значения: XXX",
    "example": "f2c0b696-2774-4d07-87a3-0a8b3a42a1a3",
    "pattern": "^[a-zA    9-]*$"
  },
  "XXX": {
    "type": "string",
    "description": "Идентификатор XXX. Регулярка проверяет допустимые значения: XXX",
    "example": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6",
    "pattern": "^[a-zA-    -]*$"
  },
  "XXX": {
    "type": "string",
    "description": "IP-адрес, с которого выполнен вход",
    "example": "XXX"
  },
  "XXX": {
    "type": "string",
    "description": "Сообщение об ошибке (если вход не удался)",
    "example": "XXX"
  },
  "XXX": {
    "type": "object",
    "description": "вложенный объект содержащий параметры сессии, забираем одно поле внутри",
    "properties": {
      "XXX": {
        "type": "string",
        "description": "Метод XXX",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
        "description": "URI перенаправления после входа",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
        "description": "Информация о согласии пользователя",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
        "description": "Идентификатор XXX",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
        "description": "имя пользователя",
        "example": "XXX",
        "pattern": "^[a-zA    ]*$. Регулярка проверяет допустимые значения:"
      },
      "XXX": {
        "type": "string",
        "description": "тип ответа OAuth",
        "example": "XXX"
      },
      "XXX": {
        "type": "string",
        "description": "тип ответа OAuth",
        "example": "XXX"
      },
      "XXX": {
```

```
        "type": "string",
        "description": "Используемый провайдер идентификации",
        "example": "XXX"
    },
    "required": ["XXX"]
},
"required": ["XXX", "XXX", "XXX", "XXX"]
}
```

## Технические требования для интеграции

Статус	Назначение	Источник(инициатор)/ Source IP/(IP-адрес / IP-сеть)	Имя источника / FQDN Source Name	Сеть источника / Source Net	Получатель / Destination IP / (IP-адрес / IP-сеть)	Имя получателя / FQDN Destination Name	Сеть получателя / Destination Net	Порт / Port	Протокол / Protocol	Комментарий
На согласовании	Сбор данных по посещаемости пользователей	XXX	XXX	XXX	XXX	XXX	XXX(DMZ)	XXX	XXX	соединение одностороннее

Диаграмма потока данных



### Принцип реализации:

- Airbyte в DMZ (DC-XXX) собирает данные с KeyCloak по защищенном соединению;
- Airbyte производит XXX через скрипт (JSON Schema + XXX);
- передает провалидированные и профильтрованные данные на HQ-XXX (у себя не сохраняет);
- с HX-XXX данные попадают на HX-XXX;