ООО "РТ МИС"

ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА.МИС 3.0

(ЕЦП.МИС 3.0)

Руководство администратора. Подсистема "Интеграция с ЕГИСЗ". Модуль "Маршрутизация запросов при взаимодействии с ЕГИСЗ" 3.0

Содержание

1 Введение

1.1 Область применения

Настоящий документ описывает порядок работы с модулем "Маршрутизация запросов при взаимодействии с ЕГИСЗ" 3.0 Единой цифровой платформы МИС 3.0 (далее – "ЕЦП.МИС 3.0", Система) для медицинских организаций, осуществляющих деятельность в сфере обязательного медицинского страхования (далее – ОМС).

1.2 Уровень подготовки администратора

К администраторам Подсистемы предъявляются следующие требования:

- Глубокое понимание Подсистемы на уровне технологий работы;
- Знание основ администрирования;
- Знание основ администрирования реляционных баз данных, поддерживающих клиент-серверный режим;
- Навыки реализации различных режимов работы операционных систем;
- Администрирование учетных записей пользователей Системы.

1.3 Перечень эксплуатационной документации, с которым необходимо ознакомиться администратору

Перед началом работы администраторам рекомендуется ознакомиться с положениями данного Руководства администратора в части своих функциональных обязанностей.

2 Назначение и условия применения

2.1 Виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации

Модуль "Маршрутизация запросов при взаимодействии с ЕГИСЗ" 3.0 для обеспечения доступа внешних МИС к сервисам ЕГИСЗ и обмена сведениями между внешними МИС.

2.2 Условия, при соблюдении которых обеспечивается применение средства автоматизации

Доступ к функциональным возможностям и данным Подсистемы реализуется посредством веб-интерфейса. Работа пользователей Подсистемы осуществляется на единой базе данных ЦОД. Подсистема доступна из любой организации (участника информационного обмена) при наличии канала связи в круглосуточном режиме.

Работа в Подсистеме выполняется через автоматизированные рабочие места персонала (в соответствии с местом работы, уровнем прав доступа к функциональным возможностям и данным Системы).

Настройка рабочего места (создание, настройка параметров работы в рамках МО, предоставление учетной записи пользователя) выполняется пользователем АРМ администратора МО. Настройка общесистемных параметров работы, конфигурация справочников выполняется пользователем АРМ администратора ЦОД.

Настройка внутрисистемных уведомлений пользователям Системы на уровне МО выполняется пользователем АРМ администратора МО. Расчет статистических показателей на основании структурированных исходных данных выполняется пользователем АРМ администратора МО.

2.3 Порядок проверки работоспособности

Для проверки работоспособности системы необходимо выполнить следующие действия:

Выполнить авторизацию в Системе и открыть АРМ.

Вызвать любую форму.

При корректном вводе учетных данных должна отобразиться форма выбора МО или АРМ, либо АРМ пользователя. При выполнении действий должно не должно отображаться ошибок, система должна реагировать на запросы пользователя, например, отображать ту или иную форму.

3 Подготовка к работе

3.1 Состав и содержание дистрибутивного носителя данных

Система передается в виде функционирующего комплекса на базе средств вычислительной техники.

Система развертывается Исполнителем.

Работа в Системе возможна через следующие браузеры (интернет-обозреватели):

– Mozilla Firefox (рекомендуется);

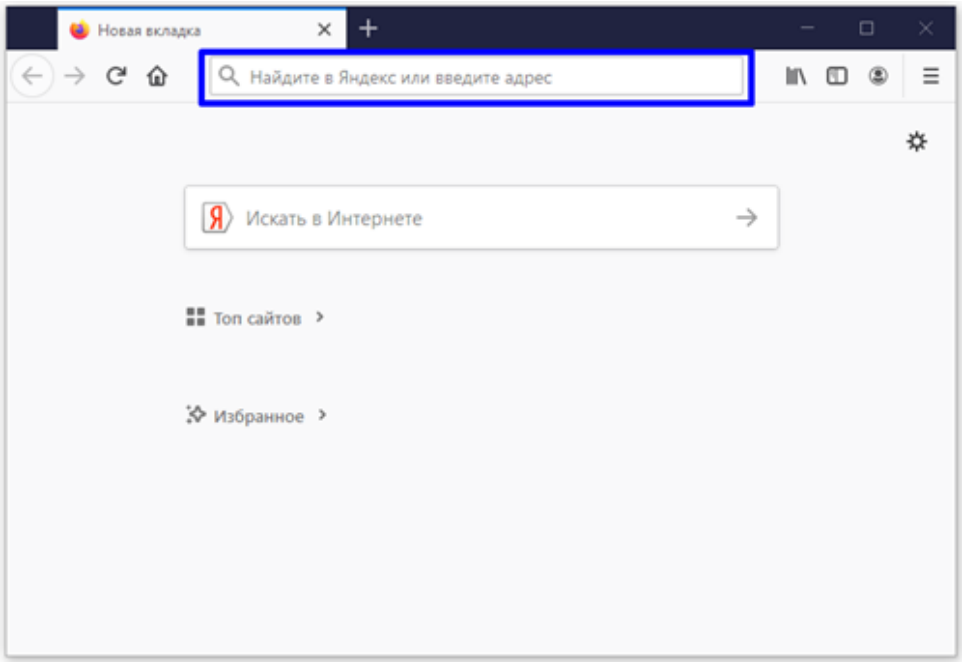
– Google Chrome.

Перед началом работы следует убедиться, что установлена последняя версия браузера. При необходимости следует обновить браузер.

3.2 Порядок запуска Системы

Для входа в Систему выполните следующие действия:

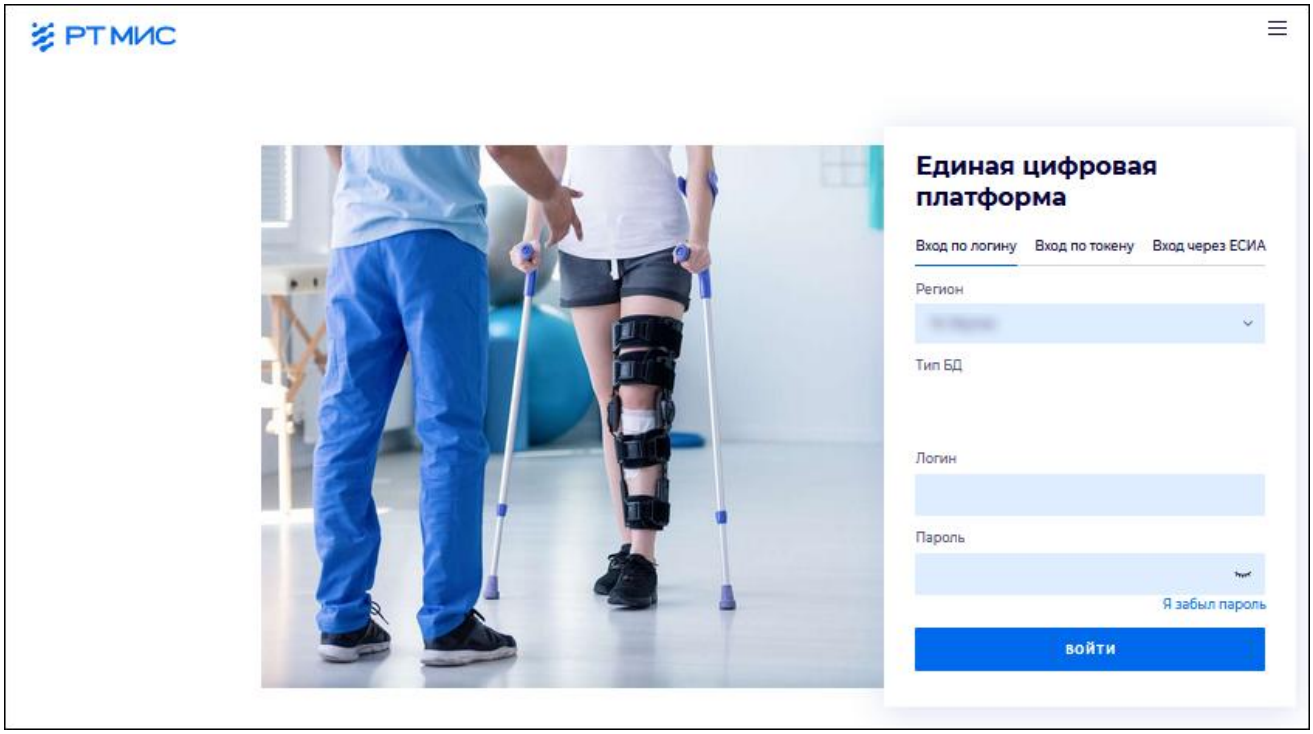
– Запустите браузер. Отобразится окно браузера и домашняя страница.



– Введите в адресной строке обозревателя адрес Системы, нажмите клавишу Enter. Отобразится главная страница Системы.

Примечание – Адрес для подключения предоставляется администратором. Если страница Системы установлена в качестве домашней страницы, то она отобразится сразу после запуска браузера.

Для удобства использования рекомендуется добавить адрес Системы в закладки интернет-обозревателя, и/или сделать страницу Системы стартовой страницей.



Авторизация в Системе возможна одним из способов:

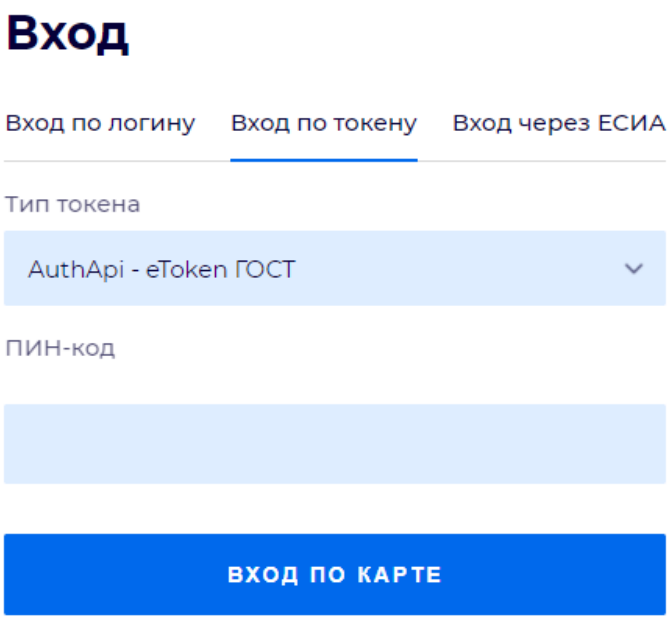
- с использованием логина и пароля;
- с помощью ЭП (выбора типа токена и ввод пароля);
- с помощью учетной записи ЕСИА.

1 способ:

- Введите логин учетной записи в поле "Имя пользователя".
- Введите пароль учетной записи в поле "Пароль".
- Нажмите кнопку "Войти".

2 способ:

- Перейдите на вкладку "Вход по токену":



– Выберите тип токена.
– Введите пароль от ЭП в поле ПИН-код/Сертификат (расположенное ниже поля "Тип токена"). Наименование поля зависит от выбранного типа токена.
– Нажмите кнопку "Вход по карте".

Примечания:

– На компьютере Пользователя предварительно должно быть установлено и запущено программное обеспечение для выбранного типа токена.
– Предварительно может потребоваться установить сертификаты пользователей администратором системы в программном обеспечении выбранного типа токена.

При неправильном вводе имени пользователя и (или) пароля отобразится соответствующее сообщение. В этом случае необходимо повторить ввод имени пользователя и (или) пароля.

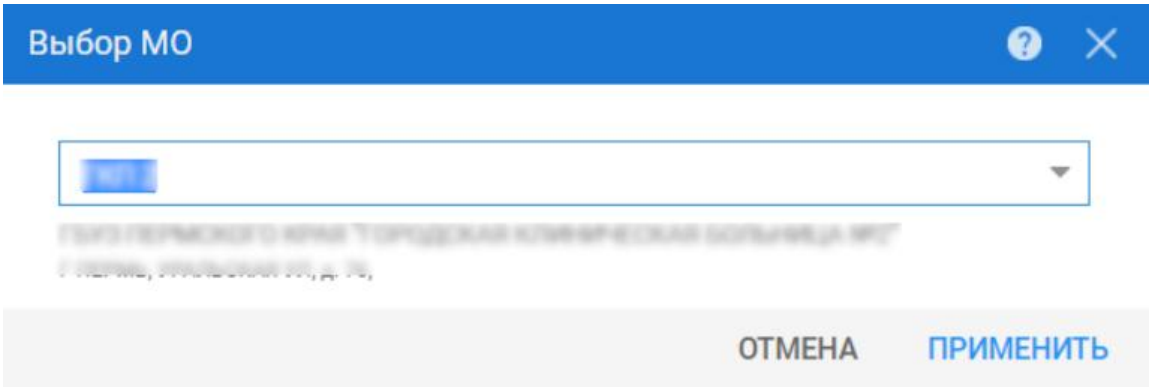
3 способ:

– Перейдите на вкладку "Вход через ЕСИА". Будет выполнен переход на страницу авторизации через ЕСИА.
– Введите данные для входа, нажмите кнопку Войти.

Примечание – Для авторизации через ЕСИА учетная запись пользователя должна быть связана с учетной записью человека в ЕСИА. Учетная запись пользователя должна быть включена в группу "Авторизация через ЕСИА".

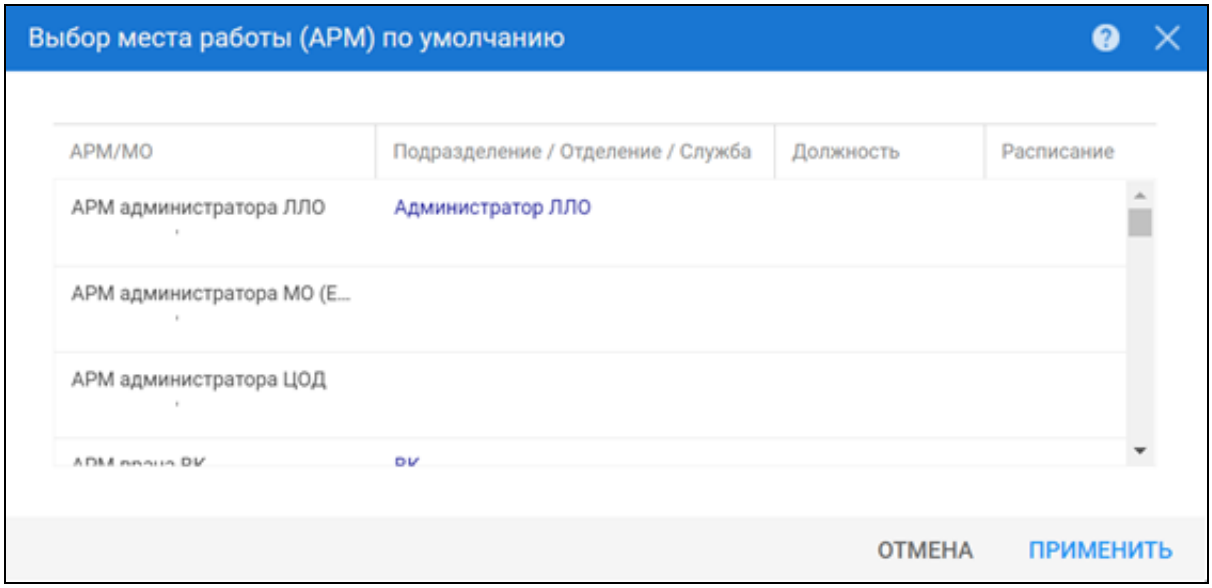
При неправильном вводе имени пользователя и (или) пароля отобразится соответствующее сообщение. В этом случае необходимо повторить ввод имени пользователя и (или) пароля.

– После авторизации одним из способов отобразится форма выбора МО.



Укажите необходимую МО и нажмите кнопку "Применить".

– Отобразится форма выбора АРМ по умолчанию.



Примечание – Форма отображается, если ранее не было выбрано место работы по умолчанию, или при входе была изменена МО. После выбора места работы, указанный АРМ будет загружаться автоматически после авторизации.

Выберите место работы в списке, нажмите кнопку "Применить". Отобразится форма указанного АРМ пользователя.

4 Модуль "Маршрутизация запросов при взаимодействии с ЕГИСЗ" 3.0

4.1 Общие указания

REST-запросы, проходящие через ИПС, должны содержать JWT-токен с подписью. Для подписи запросов должен использоваться сертификат системы-инициатора запроса, указанный при регистрации системы.

Операции при взаимодействии через тестовую/промышлен версию ИПС могут осуществляться с использованием криптографического алгоритма RSA.

Коды ошибок и результата выполнения запросов к ИПС содержатся в справочнике «Классификатор кодов сообщений интерфейса прикладных систем ЕГИСЗ» (http://nsi.rosminzdrav.ru/#!/refbook/1.2.643.5.1.13.2.1.1.693).

4.2 Требования к идентификатору ИС ЕГИСЗ

У информационной системы в случае регистрации в тестовых и рабочих версиях интеграционной подсистемы интеграции прикладных подсистем и других подсистемах ЕГИСЗ должен быть одинаковый ID. Т.е. в данных системах у информационной системы единый ID.

В случае если информационная система на момент отправки заявки на регистрацию в какой-либо версии ИПС уже зарегистрирована в другой версии ИПС, а также в другой подсистеме ЕГИСЗ, в заявке необходимо указать ID ИС, указанный при регистрации в данных системах.

В случае если информационная система на момент отправки заявки на регистрацию в какой-либо версии ИПС не зарегистрирована ни в другой версии ИПС, ни в другой подсистеме ЕГИСЗ, то ее ID будет сгенерирован СТП ЕГИСЗ и предоставлен кураторам ИС. В этом случае в заявке на регистрацию ИС поле «ID ИС» нужно оставить пустым.

ВНИМАНИЕ! В случае регистрации в другой подсистеме ЕГИСЗ после регистрации в ИПС, необходимо указывать ID, полученный в ходе регистрации в ИПС.

4.3 Описание. Асинхронное взаимодействие по REST – протоколу

Инициатором асинхронного взаимодействия выступает система-потребитель, направляя REST-запрос на адрес сервиса поставщика в ИПС. В рамках запроса, потребитель передает подписанный JWT-токен в заголовке autorization, который в дальнейшем служит для

идентификации и аутентификации потребителя (формат токена описан в п. **2.5 JWT.Token и его структура**.).

Формат передачи JWT-токена в заголовке: Authorization: Bearer <token>

Пример:

```
"Authorization:Bearer
eyJ4NWMiOlsiTUlJRHJUQ0NBcFdnQXdJQkFnSUpBUFNyeG54QTJDT0VNQTBHQ1NxR1NJYjNEUUVCQ3dVQU1HM
HhDekFKQmdOVkJBWVRBbEpWTVE4d0RRWURWUVFJREFaU2RYTnphV0V4RGpBTUJnTlZCQWNNQlV0aGVtRnVNUk
l3RUFZRFZRUUtEQWxUZFhCbGNsQnNZWFF4RlRBVEJnTlZCQXNNREZOaGJYQnNaVTl5WnlCRFFURVNNQkFHQTF
VRUF3d0pVMkZ0Y0d4bFQzSm5NQjRYRFRFNU1EY3hNakE0TXpRME0xb1hEVEl3TURjeE1UQTRNelEwTTFvd2JU
RUxNQWtHQTFVRUJoTUNVbFV4RHpBTkJnTlZCQWdNQmxKMWMzTnBZVEVPTUF3R0ExVUVCd3dGUzJGNllXNHhFa
kFRQmdOVkJBb01DVk4xY0dWeVVHeGhkREVWTUJNR0ExVUVDd3dNVTJGdGNHeGxUM0puSUVOQk1SSXdFQVlEVl
FRRERBbFRZVzF3YkdWUGNtY3dnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUFBNElCRHdBd2dnRUtBb0lCQVFDOUd
adW4vdG1SWGdoa2ZqY1RjR25XUmdKZnAvZG5BbUNZTGxmaGVGcWdVcFBrNmIwTWNFRnRuU1pySHkvbHd4eVZZ
eTkxUHFyQk95ejREbEFrSXpxVGplK1dYK1p4T04rem9kRS9udzNRK0dMWVB5VVJXaWNwMUdQc1VnRXJubUVRT
k83b0tYVlk3UVJwdmRDaTA2YXQ0MkhJMEt6K1FMM2FWeFJvMkN6Q2xjZEVvUHN2Qml6aGRudmFRdW9OM24rVS
9MS2hlOXJ2MHVPUC9PcFlMVndYb0k2aEpCOGl0NFdrMStCU3pnaTVSNHY1Uk42N0hmeVF2UnFsUGZhZFVCbFd
KUml1NnNwTHkrL0hEWTRudzFtUHl6Ny9CN3paUFArWXI4akZmUVljYjI5U2ZBRkRlWHlKc2FsSlQ3emxHcXl1
RjRNdGJJNDlGODh6M2xJY21IY0xBZ01CQUFHalVEQk9NQjBHQTFVZERnUVdCQlR6K2U5NXptUFRVWGEzRGorM
DFONkNwRTlGZGpBZkJnTlZIU01FR0RBV2dCVHorZTk1em1QVFVYYTNEaiswMU42Q3BFOUZkakFNQmdOVkhSTU
VCVEFEQVFIL01BMEdDU3FHU0liM0RRRUJDd1VBQTRJQkFRQzB1ZkRmSkUwQVJ6ZSs2UmwzVlp5Z25kakNWN3Y
2angvbS9vZUVvbytNbm5JbXkrQmw3L2pId092NnlBYVhpSWFmVmt0d1VMajhUdHJvKzhybjhaWi9vWm44RmNJ
aWorMHoxK0w5UzQrRG5Ha0JSdnVNbmxSY2l4MGFzNUhpNkZqejBDN0d5dFBpVEF2bTJQRjV5MlA2OGVZeE9HT
HdBenlFTzhEUDFxMWFhdm92dDBsd0F4YkJTQ1ZhYWZiYTVKSVlWSW9RcWo1bG9GUjBuOEo5RXFWb2w0VEZvUF
JKdnFSdEd5Q1hEWEFlWjUvV0txcG0zbEd0WXhOVEtTc2xlc2FWTGI4WUU4YWhzeWFMTUpBRld1SE5CODJVYUJ
wTkZrcWFMZDZoZDMwV0EvYXNjbmNYMW9peDdiUWFtb2dyR3ZxdWZKQlVScXgvZ1hRK3ptNWtnNjJ3Il0sImFs
ZyI6IlJTMjU2In0.eyJzdWIiOiJjYmFhZjU4ZC0zNTU1LTNkNTMtZmQ2Zi1jNTkxZGJiM2RhMDciLCJhdWQiO
iJodHRwczovL2FnLWRldi5ydC1ldS5ydS8vLy8vLy8vLy8vLy8vLy8vIiwiZXhwIjoxNTYyOTM2MzYwLC
JpYXQiOjE1NjI5MzI4ODB9.CAuo1ortLCeJRZG6QMaNoM_jPheJ5E0EMYrxapW3nc7oBSegn-
Pl7vy8BSD0cxe9M8Ve4i-GiHT6SUabitIqhM532uGlwk8M2oiaHa86c1CuOl8RMUBoCAR4kX052x-D-
MJMF2qq46BWzj3CYAKKf1EmHo853fxklycUBikncy083mGcTIdfNAEnDvPrAKj1RBKf14Q23pOx1xwWwWgBO4
gmzVcClSRVBACICRw-wi7RNHiQHwW4BwJas_jEgyjBzbPiNasc8Q1Crbq7K7AX9Le9nY9OKkK9GQHGU2-
X5RqhuaXPwM9hZDGa5tH7QQfsDG6n98RBYMwF_3D1Fj66Dg"
```

После успешной проверки, ИПС направляет запрос с токеном клиента на адрес конечной точки сервиса поставщика. В рамках соединения, сервис поставщика направляет ответ, который затем перенаправляется потребителю. Далее поставщиком в асинхронном режиме обрабатывается полученный запрос и формируется ответ. В рамках нового соединения, сервис поставщика направляет сформированный асинхронный ответ и подписанный JWT-токен, на адрес сервиса обратного вызова потребителя в ИПС. Асинхронное взаимодействие

обеспечивается стороной поставщика, благодаря ведению на своей стороне маппинга идентификаторов потребителей и адресов сервисов обратного вызова. Асинхронный ответ проходит проверку по ряду политик, указанных выше, и направляется на адрес конечной точки сервиса обратного вызова потребителя. В рамках соединения, потребитель направляет синхронный ответ, который далее перенаправляется поставщику.

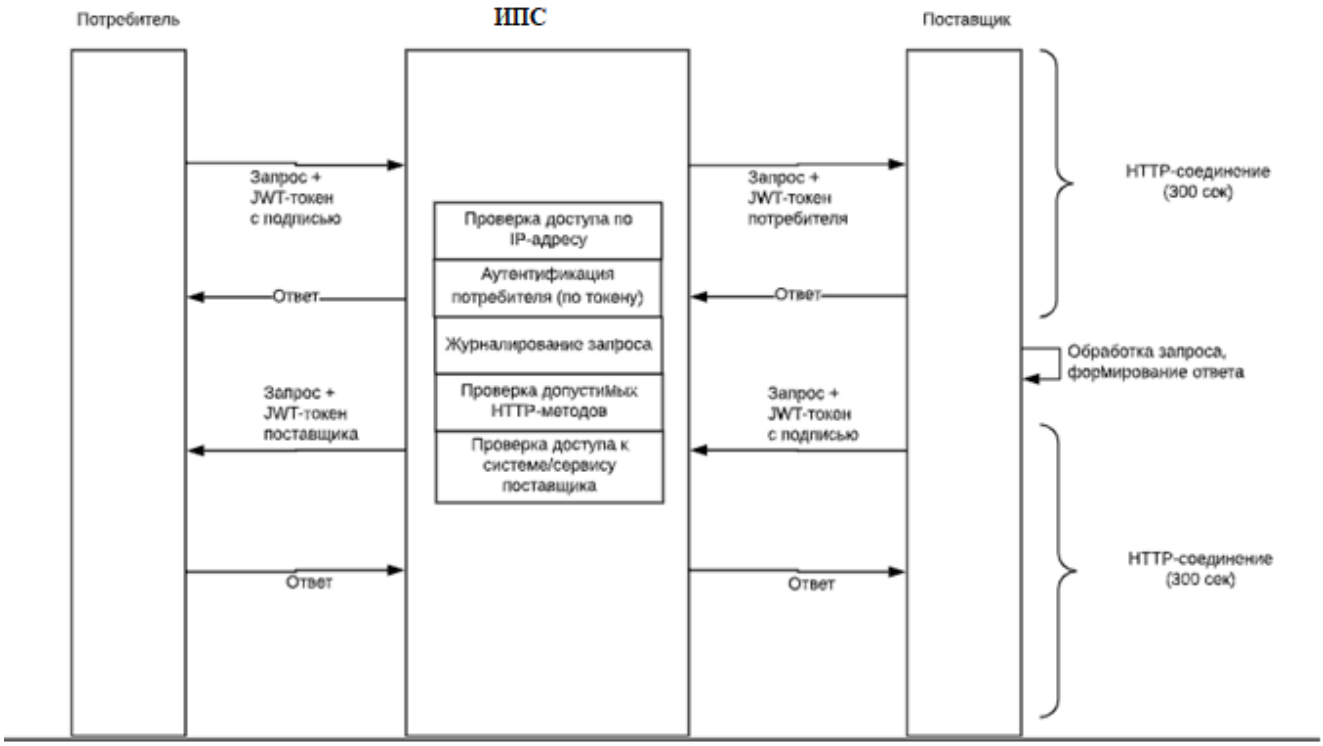


Схема 1. Схема асинхронного взаимодействия

4.4 Описание. Синхронное взаимодействие

Схема 1 и описание взаимодействия в рамках одного соединения, приведенное выше, актуальны для понимания синхронного взаимодействия.

4.5 JWT.Token и его структура

JSON Web Token (JWT) является открытым стандартом (RFC 7519), обеспечивающий передачу информации между двумя участниками в формате JSON объекта. В ИПС допускается подпись JWT-токена только посредством закрытого ключа по алгоритму RSA. В рамках взаимодействия REST-сервисов посредством ИПС, с помощью JWT-токена осуществляются функции идентификации и аутентификации системы-клиента.

4.5.1 Требования к структуре:

JSON Web Token состоит из следующих трех частей, разделенных точкой (.):

- Заголовок (header);
- Полезная нагрузка (payload);
- Подпись (signature).

Типичное представление JWT маркера: **xxxxx.yyyyy.zzzzz.**

4.5.2 Заголовок (header)

В заголовке должны присутствовать две части:

- x5c - Открытый ключ
- alg - Алгоритм подписи (RS256, RS384, RS512)

Пример заголовка:


```
{
 "x5c": [
 "MIIDrTCCApWgAwIBAgIJAPSrxnxA2COEMA0GCSqGSIb3DQEBCwUAMG0xCzAJBgNVBAYTAlJVMQ8wDQYDVQQ
IDAZSdXNzaWExDjAMBgNVBAcMBUthemFuMRIwEAYDVQQKDAlTdXBlclBsYXQxFTATBgNVBAsMDFNhbXBsZU9y
ZyBDQTESMBAGA1UEAwwJU2FtcGxlT3JnMB4XDTE5MDcxMjA4MzQ0M1oXDTIwMDcxMTA4MzQ0M1owbTELMAkGA
1UEBhMCUlUxDzANBgNVBAgMBlJ1c3NpYTEOMAwGA1UEBwwFS2F6YW4xEjAQBgNVBAoMCVN1cGVyUGxhdDEVMB
MGA1UECwwMU2FtcGxlT3JnIENBMRIwEAYDVQQDDAlTYW1wbGVPcmcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwA
wggEKAoIBAQC9GZun/tmRXghkfjcTcGnWRgJfp/dnAmCYLlfheFqgUpPk6b0McEFtnSZrHy/lwxyVYy91PqrB
Oyz4DlAkIzqTje+WX+ZxON+zodE/nw3Q+GLYPyURWicp1GPsUgErnmEQNO7oKXVY7QRpvdCi06at42HI0Kz+Q
L3aVxRo2CzClcdEoPsvBizhdnvaQuoN3n+U/LKhe9rv0uOP/OpYLVwXoI6hJB8it4Wk1+BSzgi5R4v5RN67Hf
yQvRqlPfadUBlWJRiu6spLy+/HDY4nw1mPyz7/B7zZPP+Yr8jFfQYcb29SfAFDeXyJsalJT7zlGqyuF4MtbI4
9F88z3lIcmHcLAgMBAAGjUDBOMB0GA1UdDgQWBBTz+e95zmPTUXa3Dj+01N6CpE9FdjAfBgNVHSMEGDAWgBTz
+e95zmPTUXa3Dj+01N6CpE9FdjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQC0ufDfJE0ARze+6
Rl3VZygndjCV7v6jx/m/oeEoo+MnnImy+Bl7/jHwOv6yAaXiIafVktwULj8Ttro+8rn8ZZ/oZn8FcIij+0z1+
L9S4+DnGkBRvuMnlRcix0as5Hi6Fjz0C7GytPiTAvm2PF5y2P68eYxOGLwAzyEO8DP1q1aavovt0lwAxbBSCV
aafba5JIYVIoQqj5loFR0n8J9EqVol4TFoPRJvqRtGyCXDXAeZ5/WKqpm3lGtYxNTKSslesaVLb8YE8ahsyaL
MJAFWuHNB82UaBpNFkqaLd6hd30WA/ascncX1oix7bQamogrGvqufJ
BURqx/gXQ+zm5kg62w"
 ],
 "alg": "RS256"
}
```


После кодирования заголовка в Base64Url получаем первую часть JWT маркера.

4.5.3 Полезная нагрузка (payload)

Вторая часть маркера - полезная нагрузка (payload). Требования к составу полезной нагрузки:

- sub - идентификатор системы-клиента в ИПС
- aud - получатель, для которого предназначен токен (доменное имя)

- exp - дата окончания токена в unix формате
- iat - дата время выпуска токена в unix формате

Токены с истекшим сроком действия отклоняются. Как и заголовок, полезная нагрузка кодируется в **Base64Url** и получаем вторую часть JWT маркера.

Пример полезной нагрузки:

```
      {
  "sub": "cbaaf58d-3555-3d53-fd6f-c591dbb3da07",
  "aud": "https://ag-dev.rt-eu.ru",
  "exp": 1562936360,
  "iat": 1562932880
}
```

4.5.4 Подпись (signature)

Когда у нас есть заголовок и полезная нагрузка, можно вычислить подпись. Берутся закодированные в **Base64Url** : заголовок (header) и полезная нагрузка (payload), они объединяются в строку через точку. Затем эта строка и закрытый ключ поступают на вход алгоритма, указанного в заголовке (ключ «alg»).

Пример формирования подписи с помощью алгоритма RS256:

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
    BEGIN PUBLIC KEY-----
    MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdlatRjRjogo3WojgGHFHYLugdUWAY9iR3fy4arWNA1
KoS8kVw33cJibXr8bvwUAUparCwlvdbH6dvEOfou0/gCFQsHUfQrSDv+MuSUMAe8jzKE4qW+jK+xQU9a03GUn
KHkkle+Q0pX/g6jXZ7r1/xAK5Do2kQ+X5xK9cipRgEKwIDAQAB
    -----END PUBLIC KEY-----,
    -----BEGIN RSA PRIVATE KEY-----
    MIICWwIBAAKBgQDdlatRjRjogo3WojgGHFHYLugdUWAY9iR3fy4arWNA1KoS8kVw33cJibXr8bvwUAUpa
rCwlvdbH6dvEOfou0/gCFQsHUfQrSDv+MuSUMAe8jzKE4qW+jK+xQU9a03GUnKHkkle+Q0pX/g6jXZ7r1/xAK
5Do2kQ+X5xK9cipRgEKwIDAQABAoGAD+onAtVye4ic7VR7V50DF9bOnwRwNXrARcDhq9LWNRrRGElESYYTQ6E
batXS3MCyjjX2eMhu/aF5YhXBwkppwxg+EOmXeh+MzL7Zh284OuPbkglAaGhV9bb6/5CpuGb1esyPbYW+Ty2P
C0GSZfIXkXs76jXAu9TOBvD0ybc2YlkCQQDywg2R/7t3Q2OE2+yo382CLJdrlSLVROWKwb4tb2PjhY4XAwV8d
1vy0RenxTB+K5Mu57uVSTHtrMK0GAtFr833AkEA6avx20OHo61Yela/4k5kQDtjEf1N0LfI+BcWZtxsS3jDM3
i1Hp0KSu5rsCPb8acJo5RO26gGVrfAsDcIXKC+bQJAZZ2XIpsitLyPpuiMOvBbzPavd4gY6Z8KWrfYzJoI/Q9
FuBo6rKwl4BFoToD7WIUS+hpkagwWiz+6zLoX1dbOZwJACmH5fSSjAkLRi54PKJ8TFUeOP15h9sQzydI8zJU+
upvDEKZsZc/UhT/SySDOxQ4G/523Y0sz/OZtSWcol/UMgQJALesy++GdvoIDLfJX5GBQpuFgFenRiRDabxrE9
MNUZ2aPFaFp+DyAe+b4nDwuJaW2LURbr8AEZga7oQj0uYxcYw==
    -----END RSA PRIVATE KEY-----

)
```

4.5.5 Объединим все вместе

Теперь, когда у нас есть заголовок, полезная нагрузка и подпись, мы можем построить JWT. Окончательный JWT выглядит следующим образом:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9l
IiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```