Общество с ограниченной ответственностью
«Научно-Технический Центр ПРОТЕЙ»
(ООО «НТЦ ПРОТЕЙ»)

# ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ АВТОРИЗАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ PROTEI GLOBUS-PASS

## РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА

RUS.ПАМР.50300-01 32

Санкт-Петербург
2024

| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |
|---|---|---|---|---|
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| Изм. | Лист | № докум. | Подпись | Дата |

Литера ___

**Аннотация**

Настоящий документ «Программное обеспечение безопасной авторизации и аутентификации пользователей PROTEI Globus-PASS. Руководство системного программиста» разработан на Программное обеспечение безопасной авторизации и аутентификации пользователей PROTEI Globus-PASS (далее — PROTEI Globus-PASS) производства Общества с ограниченной ответственностью «Научно-Технический Центр ПРОТЕЙ» (далее — ООО «НТЦ ПРОТЕЙ»). Настоящий документ предназначен для подачи в Минцифры России вместе с заявлением о внесении сведений о программном обеспечении PROTEI Globus-PASS в единый реестр российских программ для электронных вычислительных машин и баз данных. Описание программы содержит сведения о логической структуре и функционировании программы.

Руководство системного программиста содержит сведения для проверки, обеспечения функционирования и настройки программы.

Настоящий документ построен на основании стандартов ООО «НТЦ ПРОТЕЙ».

**СОДЕРЖАНИЕ**

# 1 Термины и сокращения

В таблице 1 приведены используемые в настоящем документе термины и сокращения.

Таблица 1 — Используемые термины и сокращения.

| Термин | Описание |
|---|---|
| 3GPP | 3rd Generation Partnership Project, Проект партнерства третьего поколения — партнерство ведущих организаций по сертификации для развития 3G–сетей |
| API | Application programming interface, дословно интерфейс программирования приложения) — программный интерфейс, то есть описание способов взаимодействия одной компьютерной программы с другими |
| LDAP | Lightweight Directory Access Protocol, «легковесный протокол доступа к каталогам» — протокол прикладного уровня для доступа к службе каталогов X.500 |
| OIDC | OpenID Connect, открытый стандарт децентрализованной системы аутентификации |

# 2 Общие сведения

## 2.1 Обозначение и наименование программы

Обозначение – RUS.ПАМР.50300-01 32.

Наименование – Программное обеспечение безопасной авторизации и аутентификации пользователей PROTEI Globus-PASS.

Краткое наименование – PROTEI Globus-PASS.

## 2.2 Программное обеспечение

Для функционирования Globus-PASS необходимо следующее программное обеспечение:

1. Операционная система:

– Astra Linux 1.7;

– Ubuntu 22.

## 2.3 Языки программирования

Языки программирования, на которых написана программа:

1. Core: GO.

2. Web: JS (React).

## 2.4 Системные требования для серверной части

Программное обеспечение готово к установке на виртуализированные вычислительные ресурсы с минимальными характеристиками от 2vCPU, RAM 2 Gb, HDD 50Gb.

### 2.5 Техническая поддержка

Техническая поддержка и дополнительное консультирование по вопросам, возникающим в процессе установки и эксплуатации изделия, осуществляются производителем и службой технической поддержки.

#### 2.5.1 Производитель

ООО «НТЦ ПРОТЕЙ»

194044, Санкт-Петербург

Большой Сампсониевский пр., д. 60, лит. А

Бизнес-центр «Телеком СПб»

Тел.: (812) 449-47-27

Факс: (812) 449-47-29

WEB: http://www.protei.ru

E-mail: sales@protei.ru

#### 2.5.2 Служба технической поддержки

ООО «НТЦ ПРОТЕЙ»

194044, Санкт-Петербург

Большой Сампсониевский пр., д. 60, лит. А

Бизнес-центр «Телеком СПб»

Тел.: (812) 449-47-27 доп. 5888 (круглосуточно)

Факс: (812) 449-47-29

WEB: http://www.protei.ru

E-mail: mobile.support@protei.ru

**Внимание!**

Перед установкой и началом эксплуатации изделия необходимо внимательно ознакомиться с паспортом изделия и эксплуатационной документацией.

Данный документ должен постоянно находиться при изделии.

# 3 Описание системы

## 3.1 Назначение системы

PROTEI Globus-PASS — программный продукт, предназначенный для управления идентификацией и управления доступом. PROTEI Globus-PASS предоставляет централизованный и надежный механизм аутентификации, авторизации и управления пользователями как для внутренних приложений и сервисов компании Протей, так и сторонних.

## 3.2 Преимущества PROTEI Globus-PASS

PROTEI Globus-PASS обладает следующими особенностями:

1. Поддержка механизма Single Sign-On (SSO), который позволяет пользователям войти во все свои приложения с единственной учетной записью.
2. Управление пользователями: предоставляет удобный интерфейс для создания, управления и аутентификации пользователей.
3. Поддержка различных протоколов аутентификации: OAuth, OpenID Connect.
4. Возможность для других приложений напрямую проходить авторизацию, используя Oauth2.0 и OIDC через внешний API.
5. Журналирование действий пользователей: выполняется в формате CEF с дальнейшей передачей в SIEM-систему.
6. Управление конфигурацией, пользователями, клиентами и другими функциями системы посредством административного вэб-интерфейса.
7. Интеграция со сторонними LDAP/AD системами.
8. Возможность получения дополнительной информации о пользователях по данным из LDAP сервера.

### 3.2.1 Функциональные возможности

PROTEI Globus-PASS выполняет функции:

1. Авторизация пользователей.
2. Назначение пользователям ролей на основе LDAP групп.

3. Подключение клиентов для авторизации по Oauth2.0. Выдача необходимых данных с помощью скачивания готового файла настроек.

4. Поддержка основных flow авторизации: Authorization Code Grant, Implicit Grant, Resource Owner Password Credentials Grant.

5. Поддержка openID connect согласно спецификации.

6. Возможность обогащения данных авторизации дополнительными данными.

7. Получение и передача дополнительных полей из LDAP.

8. Обеспечение SSO для всех клиентов, подключенных к одному PROTEI Globus-PASS.

9. Контроль времени действия пользовательской сессии с помощью access и refresh token.

10. Возможность интеграции со сторонними приложениями, поддерживающими Oauth2.0 и OIDC.

11. Настройка шаблонов привилегий для любого приложения.

12. Гранулированная настройка доступа за счет формирования ролей на основе шаблонов привилегий.

13. Суммирование привилегий ролей на основе весов доступа. *Запрет* имеет больший вес, *разрешено* средний и *не разрешено* наименьший.

14. Возможность смены пароля для пользователей.

15. Поддержка политики безопасности паролей:

– минимальная длина пароля;

– история использованных паролей;

– время действия пароля (максимально и минимальное);

– обязательная смена пароля после первой авторизации;

– блокировка учетной записи после нескольких неправильных попыток ввода пароля:

- постоянная блокировка;
- временная блокировка.

16. Отказоустойчивость за счет возможности резервирования каждой из компонент в режиме active/active.

### 3.3 Основные принципы работы

В PROTEI Globus-PASS необходимо пройти регистрацию клиентам, которые будут проходить через него авторизацию. К PROTEI Globus-PASS подключается LDAP, в котором хранятся пользователи, разделенные по группам. Для подключенного клиента (приложения) формируется шаблон и роли. В карточке клиента каждой роли назначается своя LDAP группа.

Из PROTEI Globus-PASS скачивается клиентский файл с данными для подключения к нему. Данный файл подкладывается клиенту (приложению). Полученный файл считывает библиотека (pass-lib), которая интегрируется в приложение, либо из полученного файла берутся необходимые значения и прописываются в свой конфигурационный файл.

Согласно полученным настройкам, клиент предоставляет пользователю возможность из вэб-интерфейса приложения выполнить переход для авторизации в PROTEI Globus-PASS. При нажатии на кнопку происходит перенаправление на страницу PROTEI Globus-PASS, где пользователь проходит процедуры аутентификации и авторизации. После успешного прохождения процедур в приложение возвращаются данные пользователя (логин, роли и привилегии, дополнительная информация, если была запрошена и разрешена). После чего приложение открывает доступ пользователю в свой вэб-интерфейс согласно полученным роли и привилегиям.

По мере работы приложения, периодически происходит проверка активности сессии. Если она истекла, приложение запрашивает обновленные данные: access и refresh token, а также роли и привилегии. Если сессия была оставлена пользователем, то по истечению времени жизни токенов, она будет завершена. Далее необходимо пройти процедуру авторизации повторно. Помимо этого происходит проверка на

выполнение действий, где к каждой из привилегий назначается один или список запросов.

### 3.4 Интеграция с другими системами

Схема внедрения PROTEI Globus-PASS в сеть оператора и взаимодействие с другими узлами приведена на рисунке 1.

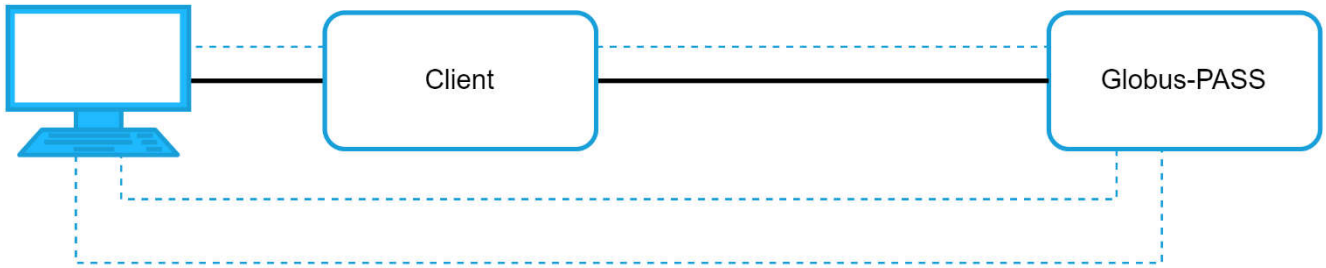


Рисунок 1 — Интеграция с элементами сети оператора

### 3.5 Диаграмма авторизации пользователя

Диаграмма с последовательностью действий и запросов PROTEI Globus-PASS при авторизации пользователя приведена на рисунке 2.

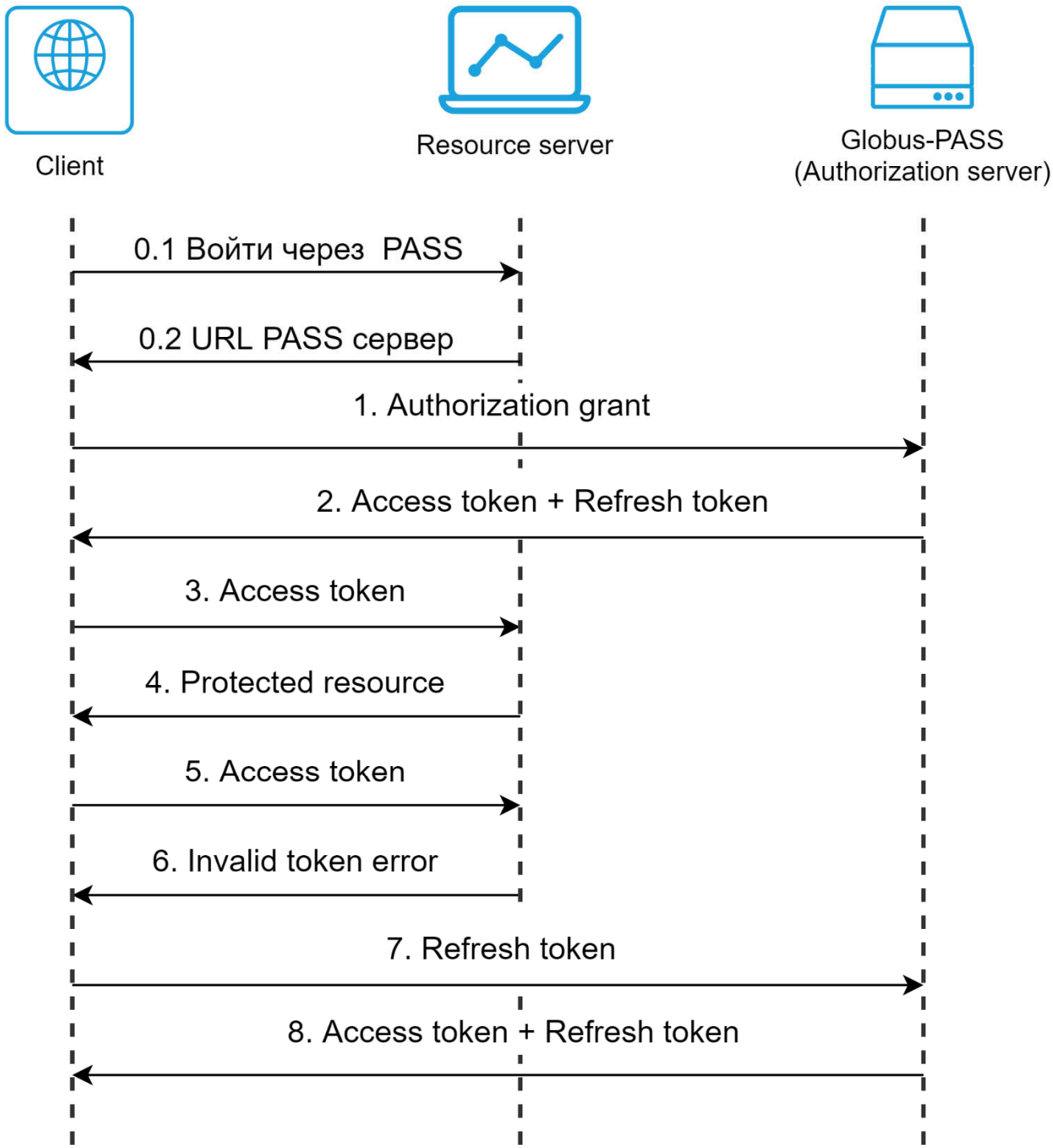


Рисунок 2 — Диаграмма авторизации пользователя

### 3.5.1 Алгоритм авторизации пользователя

1. Открыть в браузере страницу приложения, которое настроено на авторизацию через PROTEI Globus-PASS.

2. На странице приложения нажать кнопку «Войти через PASS», после чего происходит перенаправление на новое окно, где отображается страница авторизации Globus-PASS (0.1-0.2).

3. Ввести свои логин, пароль, пройти процедуру аутентификации, после чего необходимо подтвердить scope и войти в приложение.

4. После подтверждения scope происходит обмен Authorization grant (1) на Access token и Refresh token (2).

5. В процессе работы Client проверяет валидность токена у Resource server (3,4).

6. Если Access token истек (5,6), выполняется процедура обновления токена, где Refresh token обменивается на новые Access token и Refresh token (7,8).

7. Если истечет время действия Refresh token, необходимо пройти процедуру авторизации заново.

## 3.6 Управление сервисом Globus-PASS

В PROTEI Globus-PASS используются следующие директории:

1. /usr/protei/Protei-Globus/PASS/archive/ — директория для архивных файлов журналов.

2. /usr/protei/Protei-Globus/PASS/bin/ — директория для исполняемых файлов.

3. /usr/protei/Protei-Globus/PASS/bin/utils/ — директория для запускаемых скриптов, реализующих основной функционал скриптовой оболочки.

4. /usr/protei/Protei-Globus/PASS/cdr/ — директория для журналов CDR.

5. /usr/protei/Protei-Globus/PASS/config/ — директория для конфигурационных файлов.

6. /usr/protei/Protei-Globus/PASS/defaults/ — директория для значений по умолчанию.

7. /usr/protei/Protei-Globus/PASS/history/ — директория для архивных лог–файлов.

8. /usr/protei/Protei-Globus/PASS/logs/ — директория для журналов.

9. /usr/protei/Protei-Globus/PASS/scripts/ — директория для хранения скриптов.

10. /usr/protei/Backup/Protei-Globus/PASS/ — директория для резервных копий конфигураций.

Аналогичный набор директорий у сервиса API-GW, которые находятся в директории /usr/protei/Protei-Globus/API-GW

Чтобы запустить PROTEI Globus-PASS, необходимо последовательно запустить сервисы:

1. Запустить nginx:

```
service nginx restart
```

2. Запустить сервисы PROTEI Globus-PASS

```
protei-daemon start protei-globus-pass
protei-daemon start protei-globus-api-gw
protei-daemon start protei-globus-ui
```

3. Проверить успешность запуска сервисов:

```
service nginx status
protei-daemon status service-name
```

4. Остановить сервисы:

```
service nginx stop
protei-daemon stop service-name
```

# 4 Конфигурационные файлы

Параметры конфигурации задаются в файлах:

1. config.yaml директории /usr/protei/Protei-Globus/PASS/config — настройка сервера авторизации.

2. config.yaml директории /usr/protei/Protei-Globus/API-GW/config — настройка подключения клиентов по API.

3. client.yaml директории /usr/protei/Protei-Globus/API-GW/config — настройки клиента, использующего встроенную библиотеку pass_lib для авторизации через PROTEI Globus-PASS.

## 4.1 Условные обозначения

В ходе взаимодействия с сервисом происходит обмен данными определенных типов.

В таблице 2 описаны типы данных, которые применяются во время работы с сервисом.

Таблица 2 — Используемые обозначения для типов данных

| Тип | Описание |
|---|---|
| bool | Логический тип. Задает флаг. Принимает два значения, true и false |
| flag | Числовой тип. Задает флаг. Принимает два значения, 0 и 1 |
| string | Строковый тип. Задает строку. Использует буквенные, цифровые и специальные символы |
| int | Числовой тип. Задает целое 32–битное число, записанное цифрами 0–9 и знаком минуса “–”. Диапазон: от –231 до 231 – 1 |
| choice | Коллекция. Задает объект с набором полей, для каждого экземпляра должно быть определено только одно любое поле |
| object | Кортеж. Содержит фиксированное количество параметров различных типов |
| list | Список. Содержит несколько значений одного типа или структуры |
| map | Ассоциативный массив, словарь. Задает неупорядоченный набор пар ключ-значение |
| float | Числовой тип. Задает число с плавающей точкой |
| double | Числовой тип. Задает число с плавающей точкой двойной точности |
| datetime | Тип для задания даты и времени.<br>Формат по умолчанию: YYYY-MM-DD hh:mm:ss.mss, где:<br>– YYYY — год; |

| Тип | Описание |
|---|---|
| | – MM — месяц;<br>– DD — день;<br>– hh — час;<br>– mm — минута;<br>– ss — секунда;<br>– mss — миллисекунда.<br>Время задается в формате 24–часового дня |
| hex | Числовой тип. Задает целое число в формате шестнадцатеричного числа, записанного цифрами 0–9 и буквами A–F. Числу может предшествовать обозначение 0x. При отсутствии обозначения определяется как строка |
| ip | Строковый тип. Задает IP-адрес версии 4: xxx.xxx.xxx.xxx |
| None | Нулевой тип. Не задает значение, необходима инициализация объекта |
| units | Объект. Задает величину и единицы измерения:<br>– d — день;<br>– h — час;<br>– m — минута;<br>– s — секунда;<br>– ms — миллисекунда;<br>– us — микросекунда;<br>– b — биты;<br>– Kb — килобиты;<br>– Mb — мегабиты;<br>– Gb — гигабиты;<br>– Tb — терабиты;<br>– B — байты;<br>– KB — килобайты;<br>– MB — мегабайты;<br>– GB — гигабайты;<br>– TB — терабайты |

Строка типа string, регулярное выражение, задает маску, шаблон для формата данных. В таблице 3 приведено описание параметров.

Таблица 3 — Буквенные коды

| Тип | Описание |
|---|---|
| O | Optional. Опциональный параметр. Может отсутствовать в конфигурации, в таком случае используется значение по умолчанию |
| M | Mandatory. Обязательный параметр. Его отсутствие не позволяет запустить систему, а после перезагрузки конфигурации отображается сообщение об ошибке |

| Тип | Описание |
|---|---|
| X | Параметр зарезервирован и не используется при настройке конфигурации |
| P | Permanent. Параметр не переопределяется динамически, поскольку используется при запуске системы |
| R | Reloadable. Параметр, значение которого можно переопределить без перезагрузки |

### 4.2 Настройки PASS сервера (config.yaml)

Основные параметры для настройки:

1. endpoints — настройка транспортных узлов подключения для различных микросервисов.

2. pass-srv-endpoint — настройка портов доступа.

3. ldap-endpoint — настройка доступа к LDAP.

4. pass-api-srv-endpoint — настройка доступа к серверу для API запросов.

5. pass-srv:default — настройка клиентских приложений для авторизации пользователей на сервере по умолчанию (согласно OAuth2):

– ldap/endpoint — параметры блока endpoint содержат настройки древовидной структуры записей пользователя на LDAP;

– ldap/group-member-filter — параметры блока group-member-filter содержат настройки фильтрации групп, в которых состоит пользователь.

6. clients — настройка авторизации клиентов.

7. external-http-address — настройка внешних http адресов.

8. cef — общие настройки CEF-отчета.

В таблице 4 описаны параметры конфигурационного файла.

Таблица 4 — Параметры config.yaml

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| **pass-srv-endpoint** | Настройка доступа к PASS-сервера<br>Для авторизации используется протокол OAuth2 | object | | |
| listen-addr | Прослушиваемый IP-адрес для запросов микросервиса | ip | | |
| port | Порт для получения запросов | int | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| use-tls | Флаг использования протокола SSL для соединений с API-GW | bool | | |
| server-cert-file | Путь до файла сертификата *.crt<br>Примечание. Для сервера обязательно задается server-cert-file или server-key-file | string | C | |
| server-key-file | Путь до файла с ключами шифрования<br>Примечание. Для сервера обязательно задается server-cert-file или server-key-file | string | C | |
| **ldap-endpoint** | Параметры соединения с LDAP | object | | |
| service-access-url | URL для подключения к LDAP-серверу | string | | |
| port | Прослушиваемый порт для соединений с LDAP-сервером | int | | |
| use-tls | Флаг, определяющий использование протокола SSL для соединений с LDAP сервером | bool | | |
| client-cert-file | Путь до файла с сертификатом SSL. Необязательный параметр, даже если use-ssl = true | string | | |
| client-key-file | Путь до файла с ключами шифрования. Необязательный параметр, даже если use-ssl = true. | string | | |
| tls-server-name | Имя сервера в ответном сертификате для проверки. Необязательный параметр, но повышает безопасность | string | | |
| **pass-api-srv-endpoint** | | object | | |
| listen-addr | Адрес, на котором PASS-API принимает запросы от клиента | ip | | |
| use-tls | Флаг, определяющий использование шифрованного протокола HTTPS (TLS) с сертификатом для шифрования из файла /home/protei/Protei-Globus/PASS/config.selfsigned.crt | bool | | |
| server-cert-file | Путь до файла с сертификатом, обязательно либо server-cert-file, либо server-key-file для сервера | string | | |
| server-key-file | Путь до файла с ключами шифрования, обязательно либо server-cert-file, либо server-key-file для сервера | string | | |
| **telemetry-** | Настройки сервиса телеметрии OpenTelemetry. | object | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| **settings** | | | | |
| enabled | Флаг применения сервиса телеметрии | bool | | |
| host | IP-адрес хоста сервиса телеметрии | ip | | |
| port | Порт сервиса телеметрии | int | | |
| **influx-settings** | Настройка influx | object | | |
| enabled | Флаг, определяющий использовать или нет Influx базу данных | bool | | |
| url | URL для подключения к Influx | string | | |
| flush-interval | Таймаут, по которому будет происходить запись накопленных данных | unit | | |
| credentials | Настройки доступа для InfluxDB | object | | |
| username | Логин для авторизации в базе данных | string | | |
| password | Пароль для авторизации в базе данных | string | | |
| database | База данных в influx, в которую будет происходить запись | string | | |
| bucket-size | Размер буфера для накопления | int | | |
| default-tag | Тэг по умолчанию, которым будут помечены все записи | string | | |
| | key: | | | |
| | uc-office | | | |
| databases | Список подключений к базам данных | map | | |
| <name> | Имя профиля подключения к базе данных | object | | |
| host | IP адрес для подключения к базе данных | ip | | |
| port | Порт для подключения к базе данных | int | | |
| database | Имя базы данных в СУБД | string | | |
| user | Имя пользователя СУБД | string | | |
| password | Пароль пользователя СУБД | string | | |
| max-connection | Размер пула коннекций для подключения к БД | int | | |
| log-enabled | Журналирование взаимодействия с БД | bool | | |
| **pass-srv:default** | Параметры для настройки клиентских приложений по умолчанию | object | | |
| actor-services | Состоит из двух параметров:<br>– ExecutorServiceName;<br>– worker-count | map | | |
| server-endpoint | Имя Endpoint с настройками подключения к GLOBUS-PASS по OAuth | string | | |
| database | Имя профиля подключения к базе данных | string | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| api-server-endpoint | Имя Endpoint с настройками подключения к PASS-API (для конфигурирования GLOBUS-PASS) | string | | |
| request-max-size | Максимальный допустимый размер входящего запроса по OAuth | int | | |
| access-token-lifespan | Время жизни создаваемых access-token | unit | | |
| refresh-token-lifespan | Время жизни создаваемых refresh-token | unit | | |
| authorization-code-lifespan | Время жизни создаваемых authorization-code | unit | | |
| auth-session-approve-timeout | Время ожидания подтверждения доступа после аутентификации пользователя | unit | | |
| auth-cache-timeout | Время кэширования ответов от LDAP (для снижения количества запросов к LDAP) | unit | | |
| debug-enabled | Включение дополнительной отладочной информации в сообщениях об ошибках от GLOBUS-PASS | bool | | |
| **ldap** | Настройки для поиска и авторизации пользователя на LDAP | object | | |
| **endpoint1** | Имя подключения к основному LDAP | string | | |
| **endpoint2** | Имя подключения к резервному LDAP | string | | |
| dn | Корень LDAP дерева, под которым будут располагаться пользователи. Содержит параметры:<br>– ou - наименование объекта дерева. По умолчанию ou=Users;<br>– dc - контексты объекта дерева. По умолчанию dc=protei,dc=ru | list | | |
| login-key | Ключ идентификации объектов дерева. Содержит ключ, по которому будут идентифицироваться пользователи | string | | |
| mcptt-id-key | Ключ для получения mcptt-id | string | | |
| admin-bind-dn | Группа параметров для настройки политики доступа LDAP, содержат атрибуты авторизации пользователя: uid - идентификатор пользователя, ou -контекст пользователя, dc - контекст пользователя | list | O | P |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| admin-bind-password | Параметр для настройки политики доступа LDAP. Пароль для авторизации пользователя | string | O | P |
| **group-member-filter** | Настройка поиска имен групп, в которых состоит пользователь. Содержит массив настроек групп. Необязательно для указания, но необходимо для работы с ролями пользователей | object | O | P |
| group-base-dn | Корень LDAP дерева, под которым будут располагаться группы. Содержит параметры:<br>– ou - наименование объекта дерева. По умолчанию ou=Groups;<br>– dc - контексты объекта дерева. По умолчанию dc=protei,dc=ru | list | O | P |
| direct-group-member | Атрибуты, в которых указано название группы напрямую. Указывает LDAP-атрибуты пользователя, в которых хранится готовое название группы | list | | |
| | Например, атрибут пользователя memberOf=cn=group1,ou=Groups,dc=protei,dc=ru указывает на принадлежность пользователя к группе cn=group1,ou=Groups,dc=protei,dc=ru. Все остальные записи этого дерева определяют связь между атрибутом пользователя и атрибутом группы | | | |
| uid | Идентификатор пользователя группы. Связь между атрибутом пользователя uid и атрибутом группы uid. Если атрибуты группы и пользователя совпадают, то пользователь входит в группу | | | |
| gidNumber | Номер пользователя в группе. Связь между атрибутом пользователя и атрибутом группы gidNumber | | | |
| dn | Запись с параметрами атрибутов члена группы для связи с атрибутами записи о пользователе дерева пользователей | | | |
| pwpolicy-base-dn | DN по которому лежат настройки политик пароля | list | | |
| pwpolicy-attr-min-password-length | атрибут внутри DN, в котором лежит минимальная длина пароля | string | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| pwpolicy-attr-in-history | атрибут внутри DN, в котором лежит сколько раз в истории пароль повторяться не должен | string | | |
| **clients** | Секция для статической настройки параметров клиентов | map | | |
| "OSS" | Идентификатор клиента | string | | |
| secret | | string | | |
| grant-type | Тип авторизации | string | | |
| redirect-uris | | list | | |
| scopes | Запрашиваемые права: роли, привилегии, логин. Задаются в формате: ["roles", "privileges", "login"] | list | | |
| public | Признак публичного сервера доступа, true - игнорируется secret | boolean | | |
| role-mapping | Таблица ролевой модели доступа: | map | | |
| | admin: характеристики для роли Администратора,<br>– user: характеристики роли Пользователь;<br>– support: характеристики роли Инженер технической поддержки | | | |
| requested-ldap-response-attributes | | list | | |
| | o - | | | |
| | mail - | | | |
| fixed-response-attributes | Атрибуты ответа | list | | |
| | key1 - | | | |
| **external-http-address** | Настройки внешних http адресов | string | | |
| **cef** | Общие настройки CEF отчетов | object | | |
| device-vendor | Идентификатор разработчика продукта | string | | |
| device-product | Название продукта | string | | |
| device-version | Версия продукта | string | | |
| default-severity | Важность события по умолчанию | string | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| commands-info | Информация о выполняемых командах:<br>– authorize - команда авторизации;<br>– severity - важность события данной команды | object | | |
| whitelist | Белый список | list | | |
| blacklist | Черный список | list | | |
| auth-session-approve-timeout | Таймаут для сессий авторизации. | unit | | |

### 4.3 Настройки API-GW сервиса (config.yaml)

Основные параметры для настройки:

1. endpoints - транспортные узлы подключения для различных микросервисов.

2. telemetry-settings - настройки OpenTelemetry.

3. influx-settings - настройка InfluxDB.

4. api-gw-srv - настройки по умолчанию для API.

В таблице 5 описаны параметры конфигурационного файла.

Таблица 5 — Параметры config.yaml

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| version | Номер версии конфигурации | string | O | R |
| description | Описание конфигурации | string | O | R |
| **endpoints** | Транспортные точки подключения для различных микросервисов | map | | |
| <name> | Параметры подключения к микросервису: api-gw-srv-endpoint / pass-api-srv-endpoint / oss-api-srv-endpoint | object | O | P |
| service-access-url | URL, от которого разрешен доступ к микросервису | ip/string | | |
| listen-addr | Прослушиваемый IP-адрес для запросов микросервиса | ip | | |
| port | Порт для получения запросов | int | | |
| use-tls | Флаг использования протокола SSL для соединений с API-GW | bool | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| server-cert-file | Путь до файла сертификата *.crt.<br>**Примечание**: для сервера обязательно задается server-cert-file или server-key-file | string | C | |
| server-key-file | Путь до файла с ключами шифрования.<br>Примечание: для сервера обязательно задается server-cert-file или server-key-file | string | C | |
| **telemetry-settings** | Настройки сервиса телеметрии OpenTelemetry | object | | |
| enabled | Флаг применения сервиса телеметрии | bool | | |
| host | IP-адрес хоста сервиса телеметрии | ip | | |
| port | Порт сервиса телеметрии | int | | |
| **influx-settings** | Настройка системы управления базами данных InfluxDB | object | | |
| enabled | Флаг применения InfluxDB | bool | | |
| url | URL для InfluxDB | string | | |
| flush-interval | Период между записями накопленных данных в базу | units | | |
| credentials | Настройки доступа для InfluxDB | object | | |
| username | Логин для авторизации в базе данных. | string | | |
| password | Пароль для авторизации в базе данных | string | | |
| database | Имя используемой базы данных в InfluxDB | string | | |
| bucket-size | Размер буфера накопления, в байтах | int | | |
| default-tag | Параметры тега по умолчанию, добавляемого всем записям | string | | |
| key | Имя тега | string | | |
| value | Значение тега | Any | | |
| databases | Список подключений к базам данных | map | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| <name> | Имя профиля подключения к базе данных | object | | |
| host | IP адрес для подключения к базе данных | ip | | |
| port | Порт для подключения к базе данных | int | | |
| database | Имя базы данных в СУБД | string | | |
| user | Имя пользователя СУБД | string | | |
| password | Пароль пользователя СУБД | string | | |
| max-connection | Размер пула коннекций для подключения к БД | int | | |
| log-enabled | Журналирование взаимодействия с БД | bool | | |
| **api-gw-srv** | Параметры микросервисов API-GW | map | | |
| <name> | Параметры микросервиса <name> | object | | |
| actor-services | Параметры служб | map | | |
| <ExecutorServiceName> | Имя службы, работающей с API-GW | string | | |
| worker-count | Количество выделенных обработчиков | int | | |
| <WebSocketSessionName> | Название сессии по WebSocket | string | | |
| worker-count | Количество выделенных обработчиков | int | | |
| database | Имя точки подключения к базе данных | string | | |
| use-in-memory-db | Хранить данные в оперативной памяти вместо базы данных | bool | | |
| server-endpoint | Имя точки подключения к GLOBUS-API-GW по протоколу HTTP | string | | |
| server-cert-skip-verify | Флаг пропуска процедуры верификации сертификата, т.е. проверки всей цепочки центров сертификации | bool | | |
| pass-api-client-endpoints | Список с именами транспортных точек с настройками подключения к PROTEI Globus-PASS | list | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| request-max-size | Максимальный размер запроса, в байтах. | int | | |
| pass-client-file-path | Путь до файла с настройками клиента PASS-сервера, вынесенный в отдельную директорию.<br>**Примечание:** если не задан, то используется client.yaml в той же директории, где и config.yaml | string | O | |
| oss-api-client-endpoints | Список с именами транспортных точек подключения к GLOBUS-OSS | list | | |
| websocket-session-alive-timeout | Время жизни сессии при использовании WebSockets | units | | |
| websocket-compress | Флаг сжатия сообщений при использовании WebSockets | bool | | |
| nats-broker | Имя профиля с настройками брокера сообщений NATS | string | | |
| **cef** | Общие настройки CEF-отчетов | object | | |
| device-vendor | Идентификатор разработчика продукта | string | | |
| device-product | Название продукта | string | | |
| device-version | Версия продукта | string | | |
| default-severity | Важность события по умолчанию | int | | |
| commands-info | Параметры команд | [object] | | |
| <command> | Параметры команды <command_name>.<br>Формат: <command>: severity: <severity> | object | | |
| severity | Важность события по умолчанию | int | | |
| whitelist | Белый список событий | [string] | | |
| blacklist | Черный список событий | [string] | | |
| **broker** | Настройка параметров брокеров сообщений | [object] | | |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| nats | Перечень параметров брокера сообщений NATS | object | | |
| <name> | Имя профиля | object | | |
| host | IP-адрес или URL хоста для подключения | ip/string | | |
| port | Порт хоста для подключения | int | | |

### 4.4 Настройки API-GW сервиса (client.yaml)

В файле задаются настройки клиента, использующего встроенную библиотеку pass lib для авторизации через PROTEI Globus-PASS.

В таблице 6 описаны параметры конфигурационного файла.

Таблица 6 — Параметры client.yaml

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| auth-url | Адрес для авторизации на PASS | string | M | P |
| scopes | Основные параметры клиента для авторизации: имя клиента, роли клиента, привилегии, логин | [string] | M | P |
| response-type | Тип авторизации, разрешенный приложению на PASS | string | M | P |
| client-id | Идентификатор клиента, присвоенный на PASS | string | M | P |
| secret | Пароль, присвоенный на PASS | string | M | P |
| token-url | Адрес для обновления ключей | string | O | P |
| modify-password-url | Адрес для изменения пароля | string | O | P |
| revoke-url | Адрес для освобождения токена | string | O | P |
| external-http-address | Внешний адрес для перенаправления на PASS | string | O | P |
| session-auth-timeout | Время ожидания подтверждения авторизации | units | O | P |
| session-inactivity-timeout | Время ожидания активности до прекращения сессии.<br>**Примечание:** также время жизни токена refresh-token | units | O | P |
| allow_roles | Перечень доступных ролей | [string] | O | P |

| Параметр | Описание | Тип | O/M | P/R |
|---|---|---|---|---|
| callback-path | Адрес, по которому ожидается ответ на авторизацию | string | O | P |

## Лист регистрации изменений

| Изм | Номера листов (страниц) | | | | Всего листов (страниц) в док. | № документа | Входящий № сопроводи-тельного докум. и дата | Подпись | Дата |
|---|---|---|---|---|---|---|---|---|---|
| | Заме-ненных | Изме-ненных | Новых | Анну-лиро-ванных | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| Изм. | Лист | № докум. | Подпись | Дата |