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

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ АВТОРИЗАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ PROTEI GLOBUS-PASS

ОПИСАНИЕ ПРОГРАММЫ

RUS.ПАМР.50300-01 13

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. Описание программы» 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.

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
SSO	Single Sign-On, Технология единого входа — способ аутентификации, при котором пользователь входит один раз, а затем получает доступ к нескольким связанным приложениям или системам без необходимости дополнительной авторизации

2 Общие сведения

2.1 Обозначение и наименование программы

Обозначение – RUS.ПАМР.50300-01 13.

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.

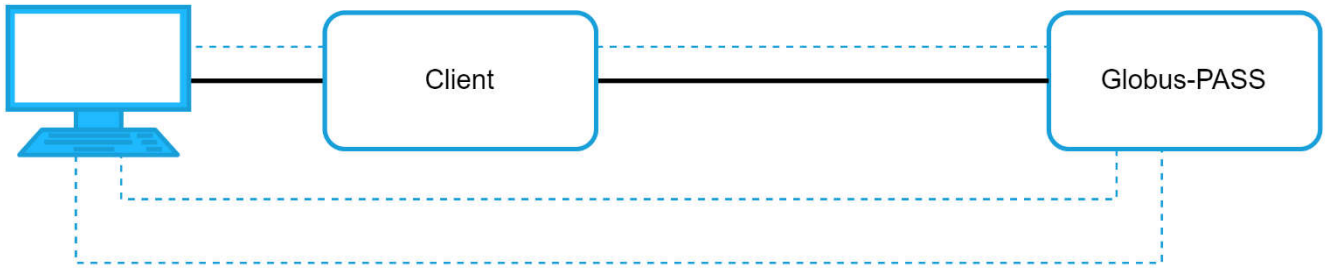

Рисунок 1 — Интеграция с элементами сети оператора

3.5 Диаграмма авторизации пользователя

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

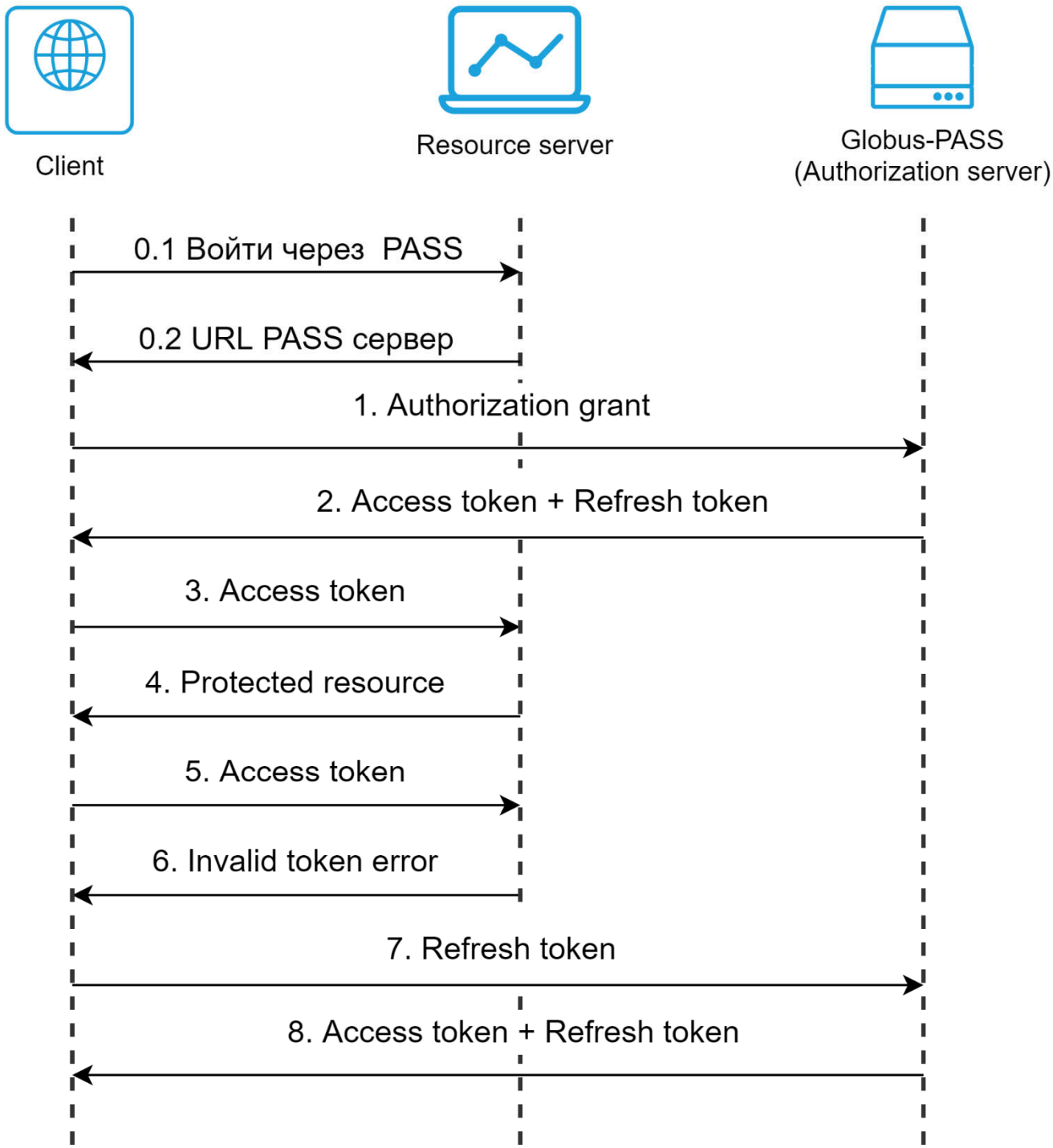

Рисунок 2 — Диаграмма авторизации пользователя

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.

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в док.	№ документа	Входящий № сопроводительного докум. и дата	Подпись	Дата
	Замененных	Измененных	Новых	Аннулированных					

Изм.	Лист	№ докум.	Подпись	Дата