External Authentication

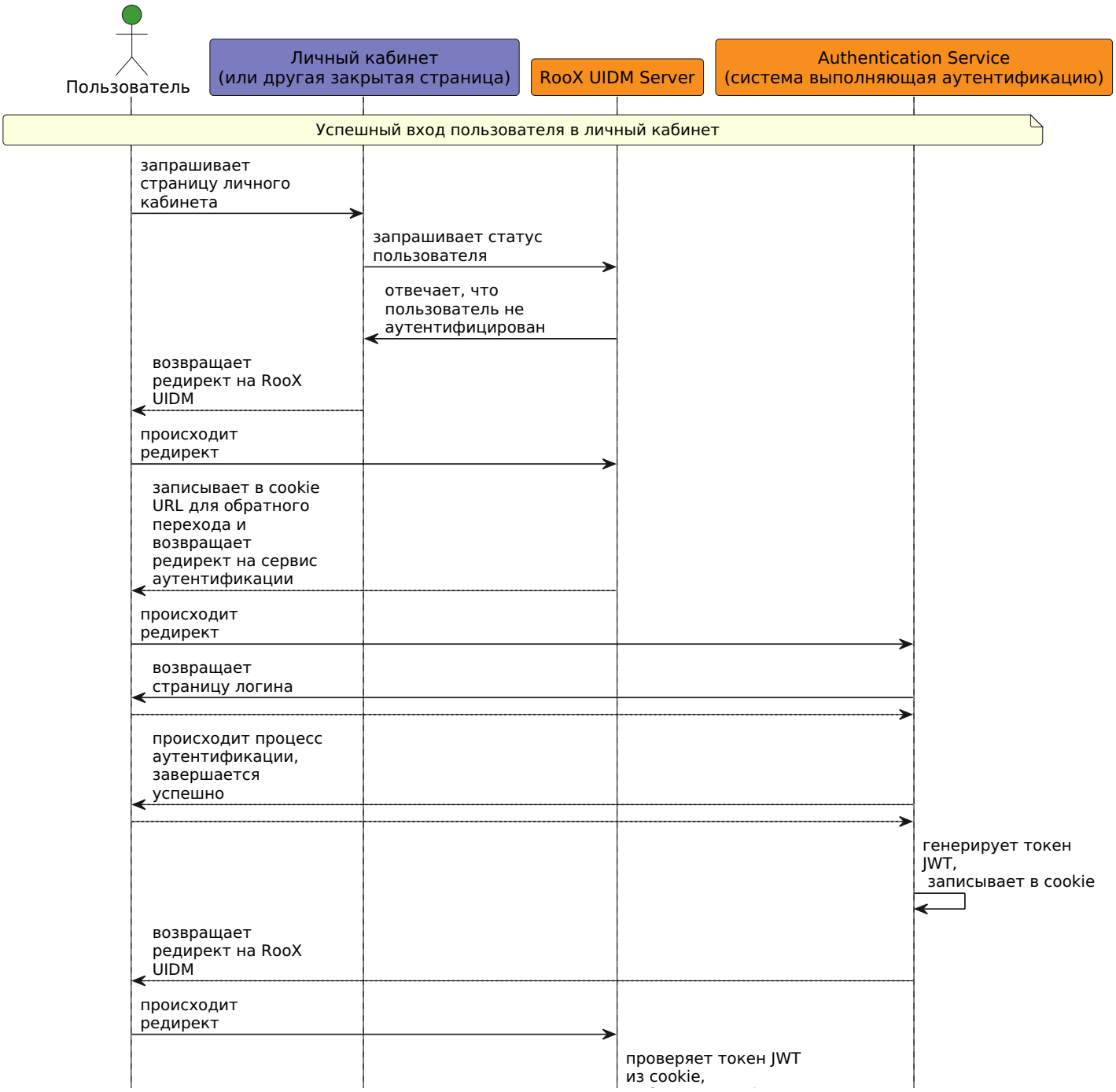
Оглавление

Аутентификация в RooX UIDM через внешнюю систему

Схема аутентификации

Аутентификация в RooX UIDM через внешнюю систему

Схема аутентификации



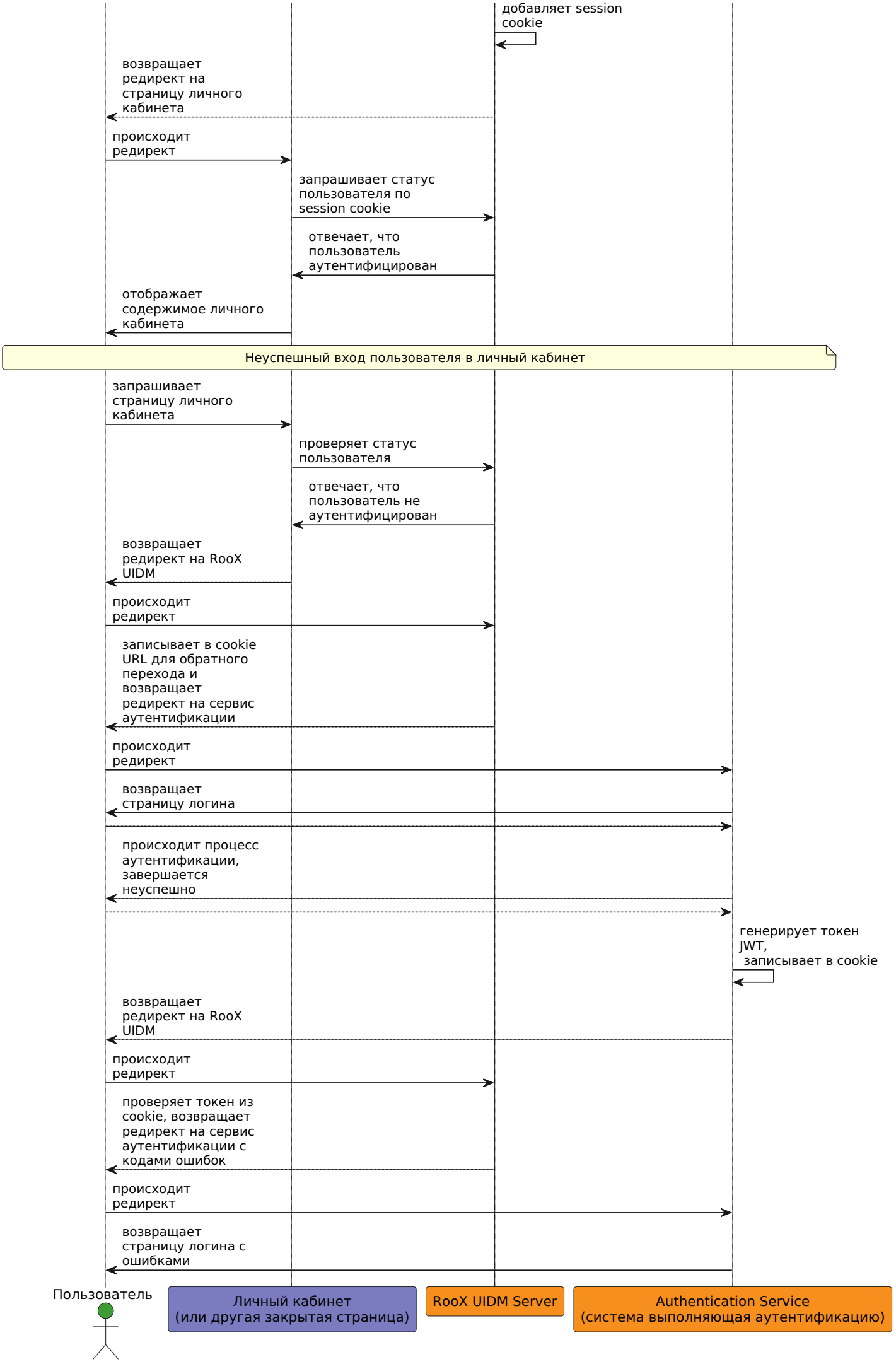

добавляет session cookie
возвращает редирект на страницу личного кабинета
происходит редирект
запрашивает статус пользователя по session cookie
отвечает, что пользователь аутентифицирован
отображает содержимое личного кабинета
Неуспешный вход пользователя в личный кабинет
запрашивает страницу личного кабинета
проверяет статус пользователя
отвечает, что пользователь не аутентифицирован
возвращает редирект на RooX UIDM
происходит редирект
записывает в cookie URL для обратного перехода и возвращает редирект на сервис аутентификации
происходит редирект
возвращает страницу логина
происходит процесс аутентификации, завершается неуспешно
генерирует токен JWT, записывает в cookie
возвращает редирект на RooX UIDM
происходит редирект
проверяет токен из cookie, возвращает редирект на сервис аутентификации с кодами ошибок
происходит редирект
возвращает страницу логина с ошибками
Пользователь
Личный кабинет (или другая закрытая страница)
RooX UIDM Server
Authentication Service (система выполняющая аутентификацию)

Рисунок 1. Аутентификация пользователя по логину/паролю через RooX UIDM External JWT Login Module

Логин Модуль ExternalJwtLoginModule

Модуль делегирует процесс аутентификации некоторой внешней системе путем редиректа на ее адрес Внешняя система может использовать любую цепочку аутентификации, после чего результат отправить редиректом обратно в RooX UIDM

Интеграция

RooX UIDM → External Auth Service

Задать настройку com.rooxteam.federation.authentication.baseUrl входной точкой логина во внешней системе. по этому адресу будут приходить GET запросы для аутентификации.

External Auth Service → RooX UIDM

В случае успешной аутентификации нужно сохранить имя пользователя и справочную информацию в виде зашифрованного токена (JWT) и записать в cookie из настройки com.rooxteam.federation.authentication.cookie.name (по умолчанию iPlanetDirectoryPro), время жизни токена должно быть несколько секунд. В случае неуспешной аутентификации нужно передать токен без информации о пользователе. В cookie из com.rooxteam.federation.authentication.backUrlCookie (по умолчанию sso_goto) должен быть записан обраный URL RooX UIDM, к этому URL необходимо добавить GET-параметр из com.rooxteam.federation.authentication.backStatusParam (по умолчанию auth_status) о статусе аутентификации (SUCCESS) и по полученному URL выполнить редирект.

Настройки

- com.rooxteam.federation.authentication.decryptor.key - Ключ расшифровки JWT токена
- com.rooxteam.federation.authentication.baseUrl - URL внешней системы аутентификации
- com.rooxteam.federation.authentication.backUrlCookie - Имя Cookie где находится URL для обратного редиректа в RooX UIDM
- com.rooxteam.federation.authentication.backStatusParam - Имя GET-параметра, в который внешняя система должна передать статус аутентификации
- com.rooxteam.federation.authentication.cookie.name - Имя Cookie в которой передается JWT
- com.rooxteam.federation.authentication.cookie.domain - Домен Cookie в которой передается JWT
- com.rooxteam.federation.authentication.cookie.path - Путь Cookie в которой передается JWT