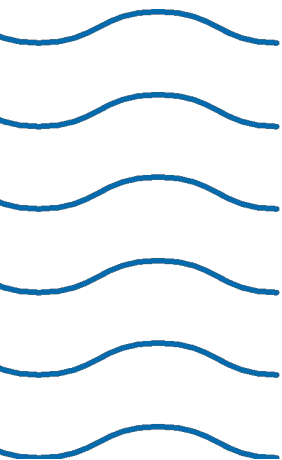


OAuth 2.0 introduction

Theory and code examples with Spring Boot



\$ whoami

Nemanja Vasic

<https://github.com/GoodbyePlanet>

Topics



What is OAuth 2.0, and what problems does it solve



How it works, and what is it good for



OAuth 2.0 basic concepts



Basic OAuth 2.0 flows for redeeming an access token - examples



Code examples

What is OAuth 2.0?

What is delegated authorization problem?

Authorization vs Authentication

OIDC (OpenID connect)

OIDC

OAuth 2.0

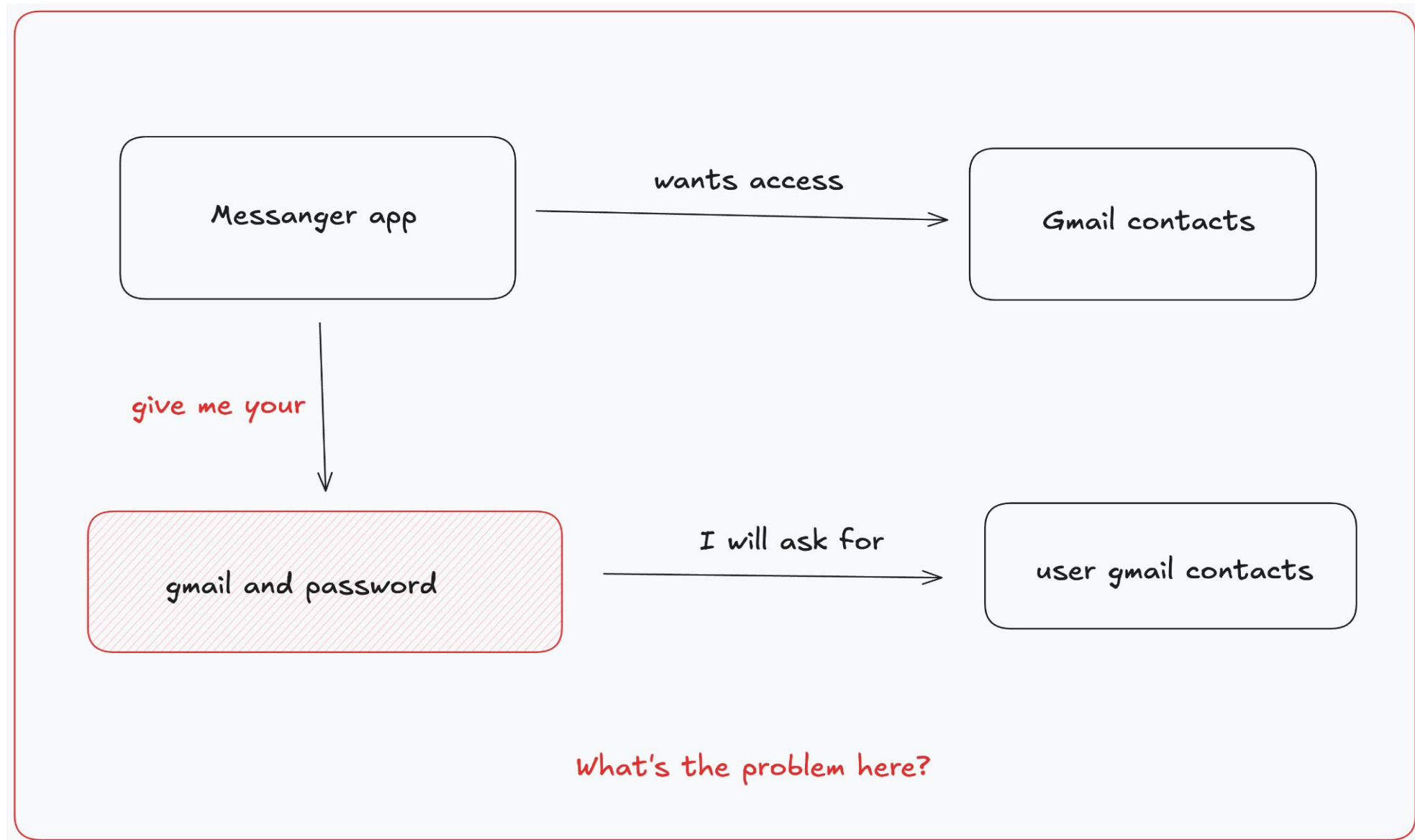
OAuth 2.0

- getting access to API
- getting access to user data present in other systems

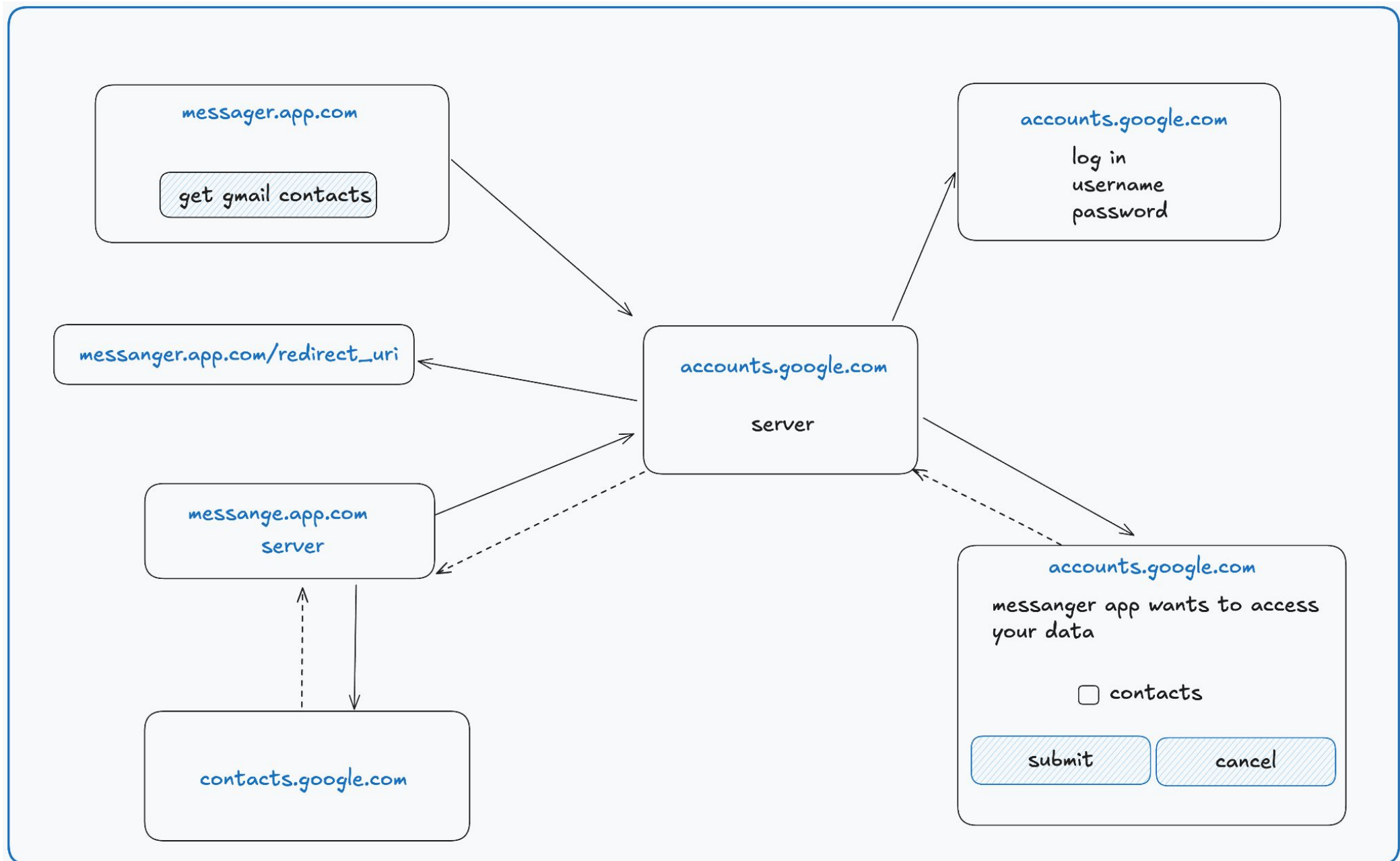
OIDC

- logging user
- getting user details
- making user details available in other systems

Before OAuth 2.0

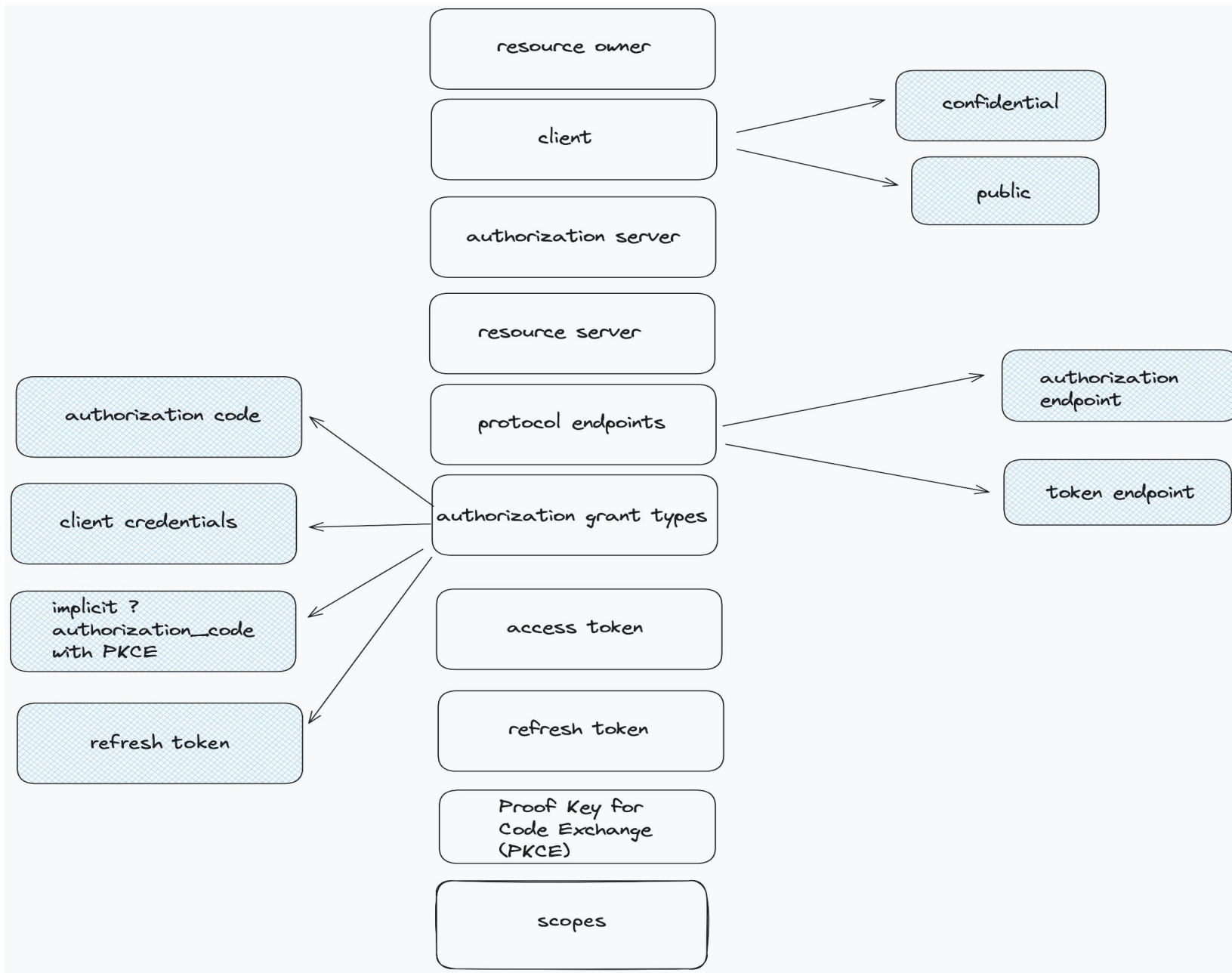


How it works with OAuth 2.0

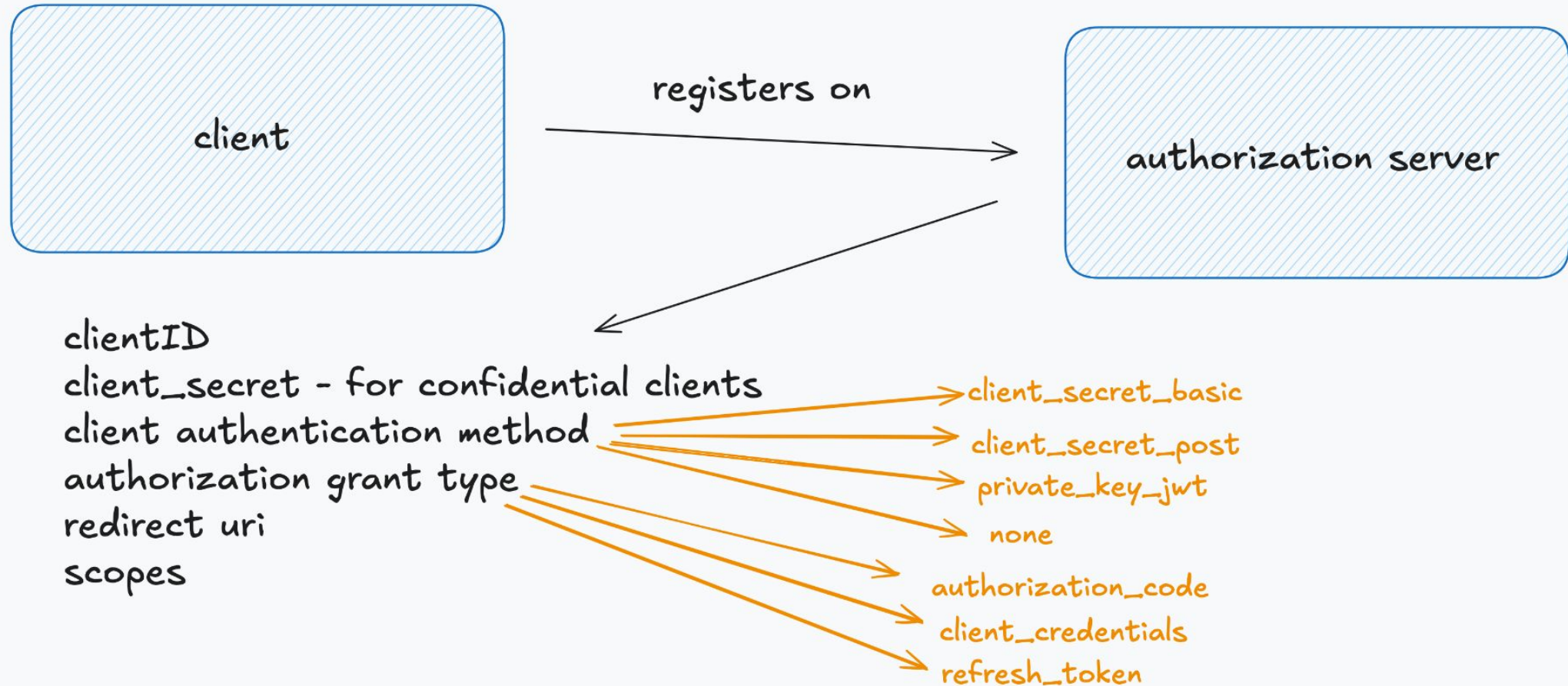


CORE CONCEPTS (ROLES)

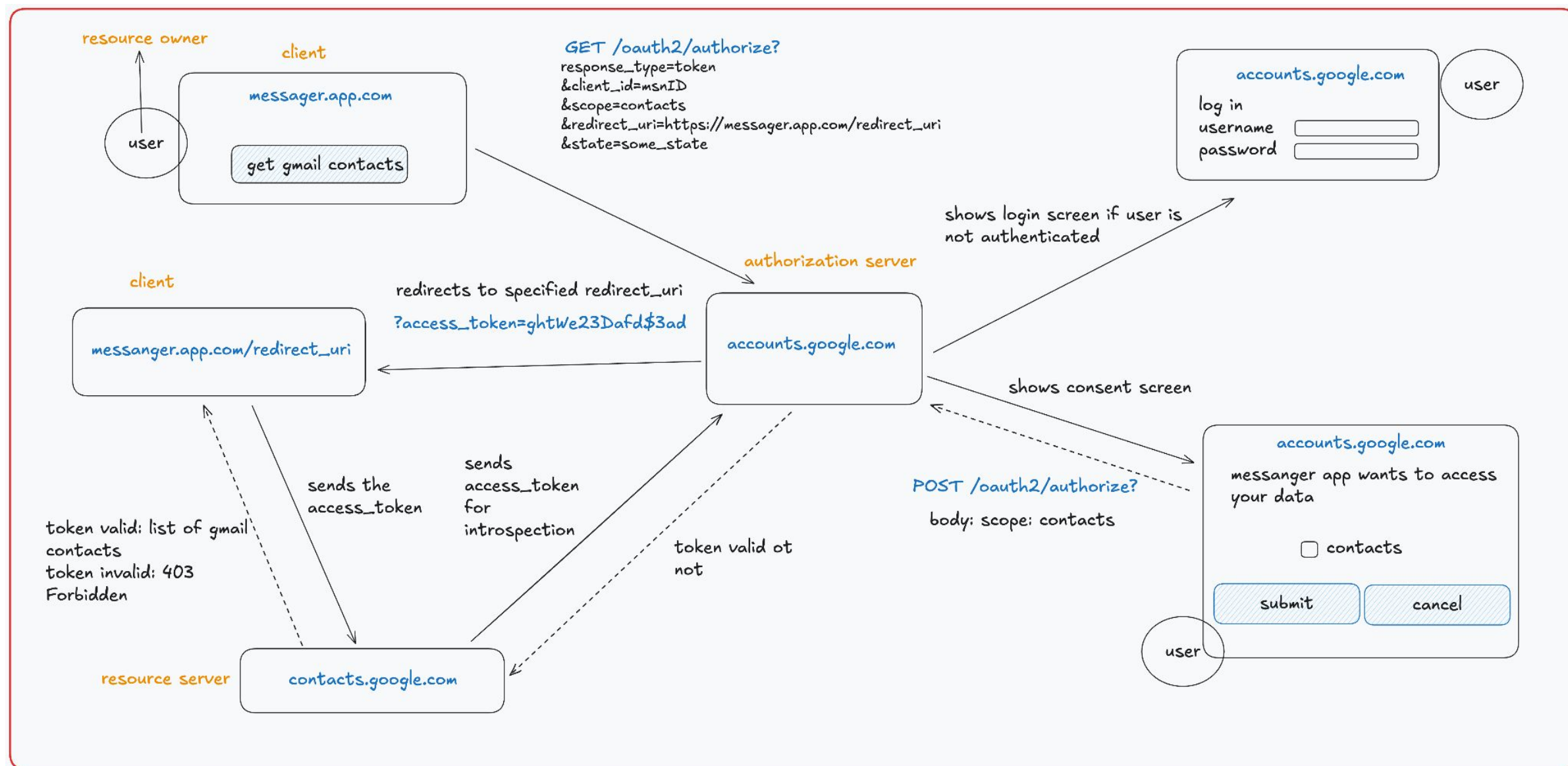
<https://datatracker.ietf.org/doc/html/rfc6749#section-1.1>



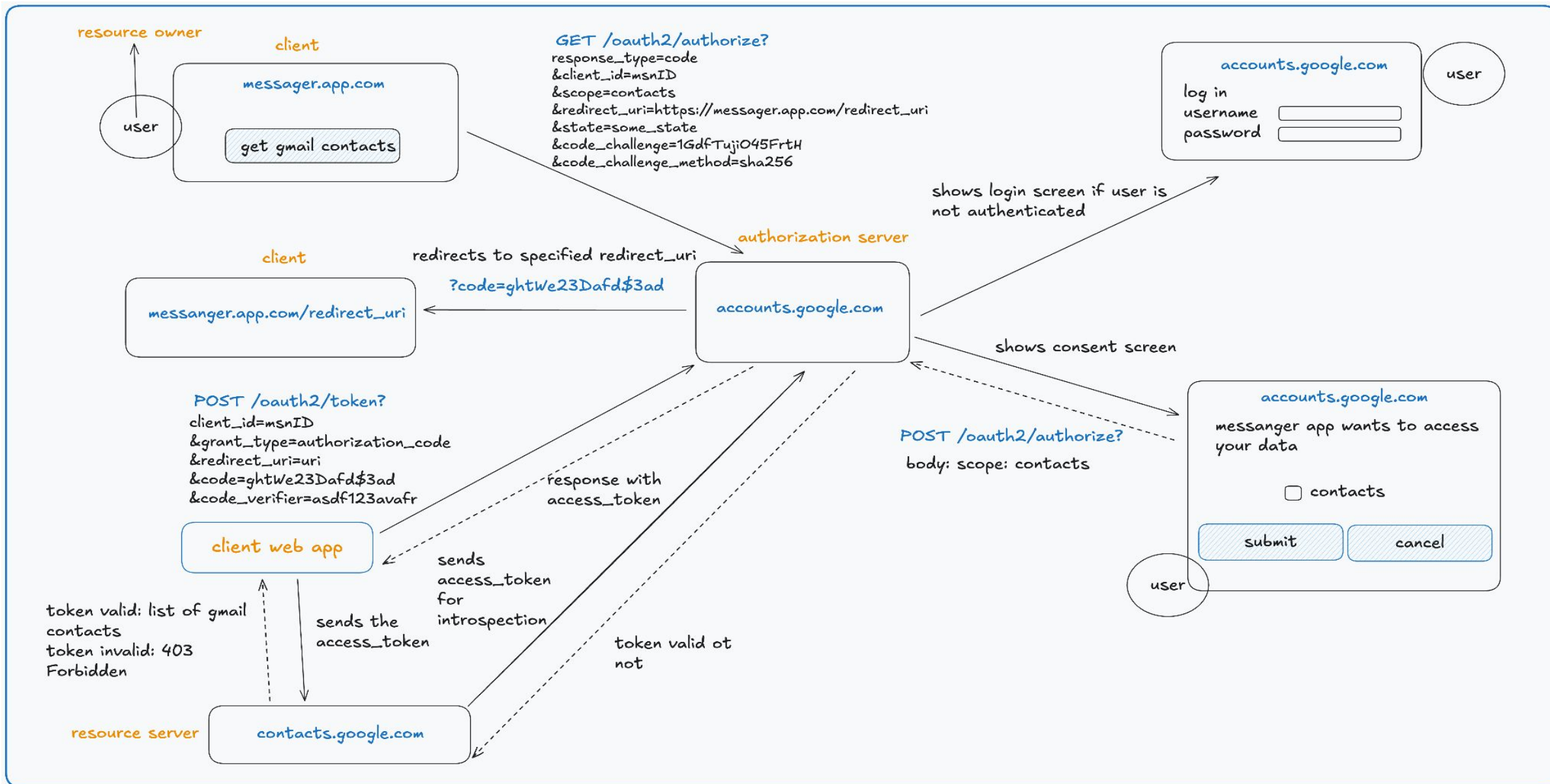
Client registration on Authorization Server



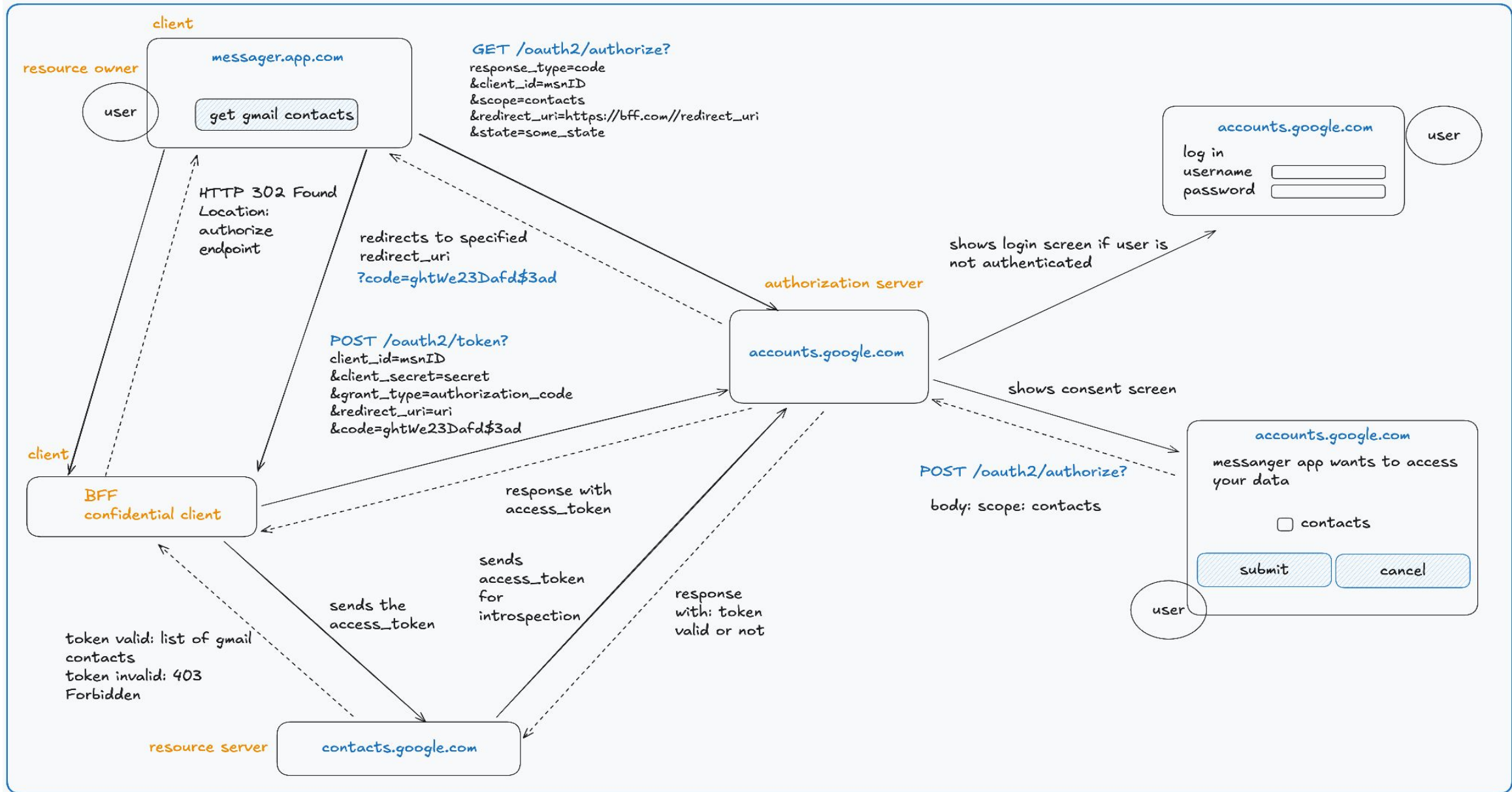
IMPLICIT Flow for PUBLIC client - Deprecated



Authorization code flow with PKCE (Proof Key for Code Exchange) - Recommended approach



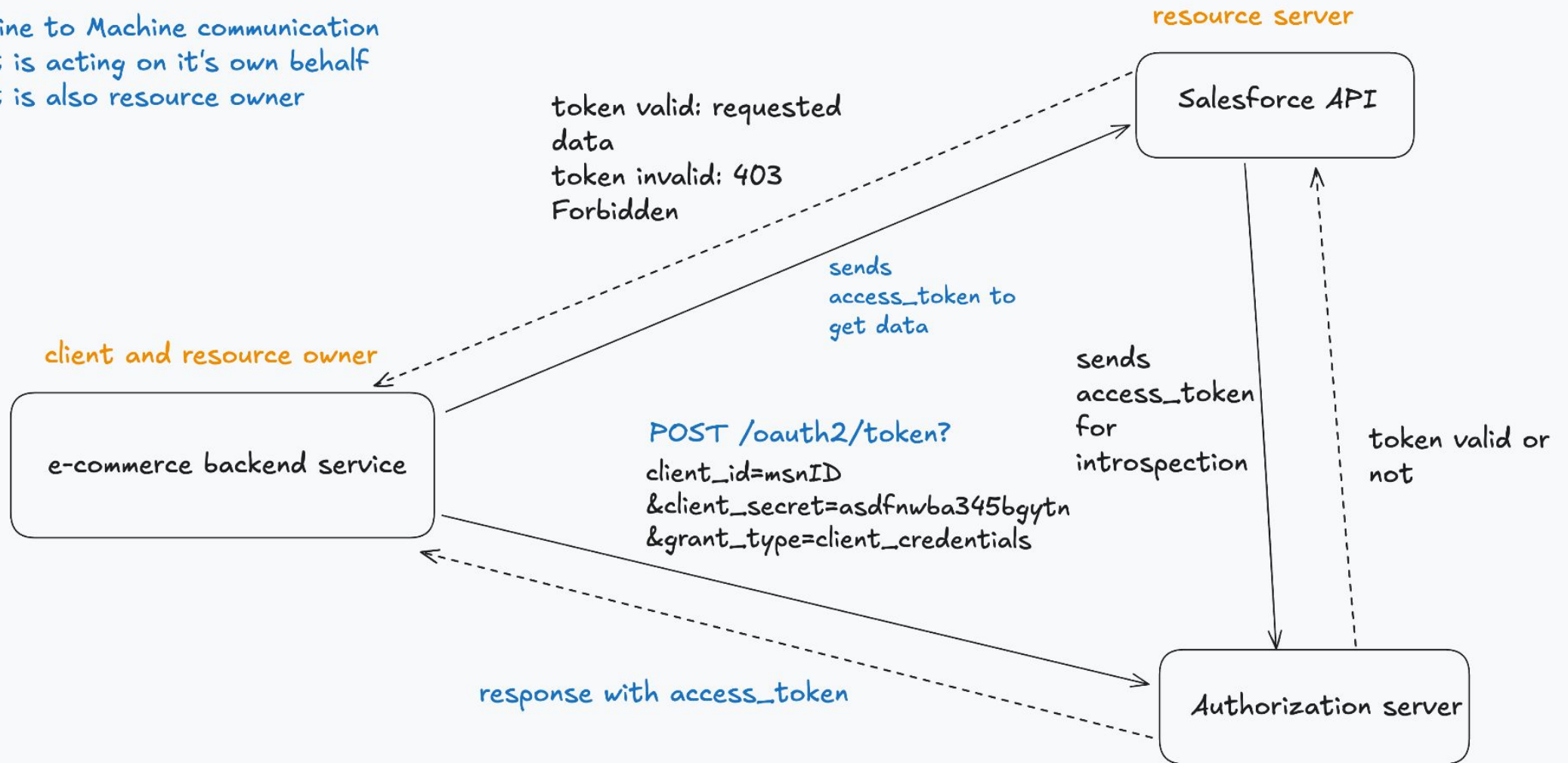
Authorization code flow with Confidential client (BFF approach) - Current best practice



Client credentials flow



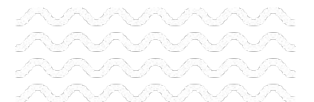
- Machine to Machine communication
- client is acting on it's own behalf
- client is also resource owner





Code example

<https://github.com/GoodbyePlanet/spring-security-friday-talk>





Q&A

