

IdentityServer

Thanh Tran – TA – 06 2020

Agenda

- Introduction
- OAuth 2.0
- IdentityServer4
- Demo
- Q&A



Introduction

The early stage of era



`select * from users where
name='thanh' and pass='123456'`

The delegated authorization problem



Are your friends already on Yelp?

Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite! And don't worry, we don't keep your email password or your friends' addresses. We loathe spam, too.

Your Email Service



Your Email Address

(e.g. bob@gmail.com)

Your Gmail Password

(The password you use to log into your Gmail email)

[Skip this step](#)

Check Contacts

The Facebook login page


Step 1
Find Friends

Step 2
Profile Information

Step 3
Profile Picture

Are your friends already on Facebook?


Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.


 Gmail

Your Email:


Email Password:

Find Friends


 Facebook will not store your password.

 Yahoo!

Find Friends

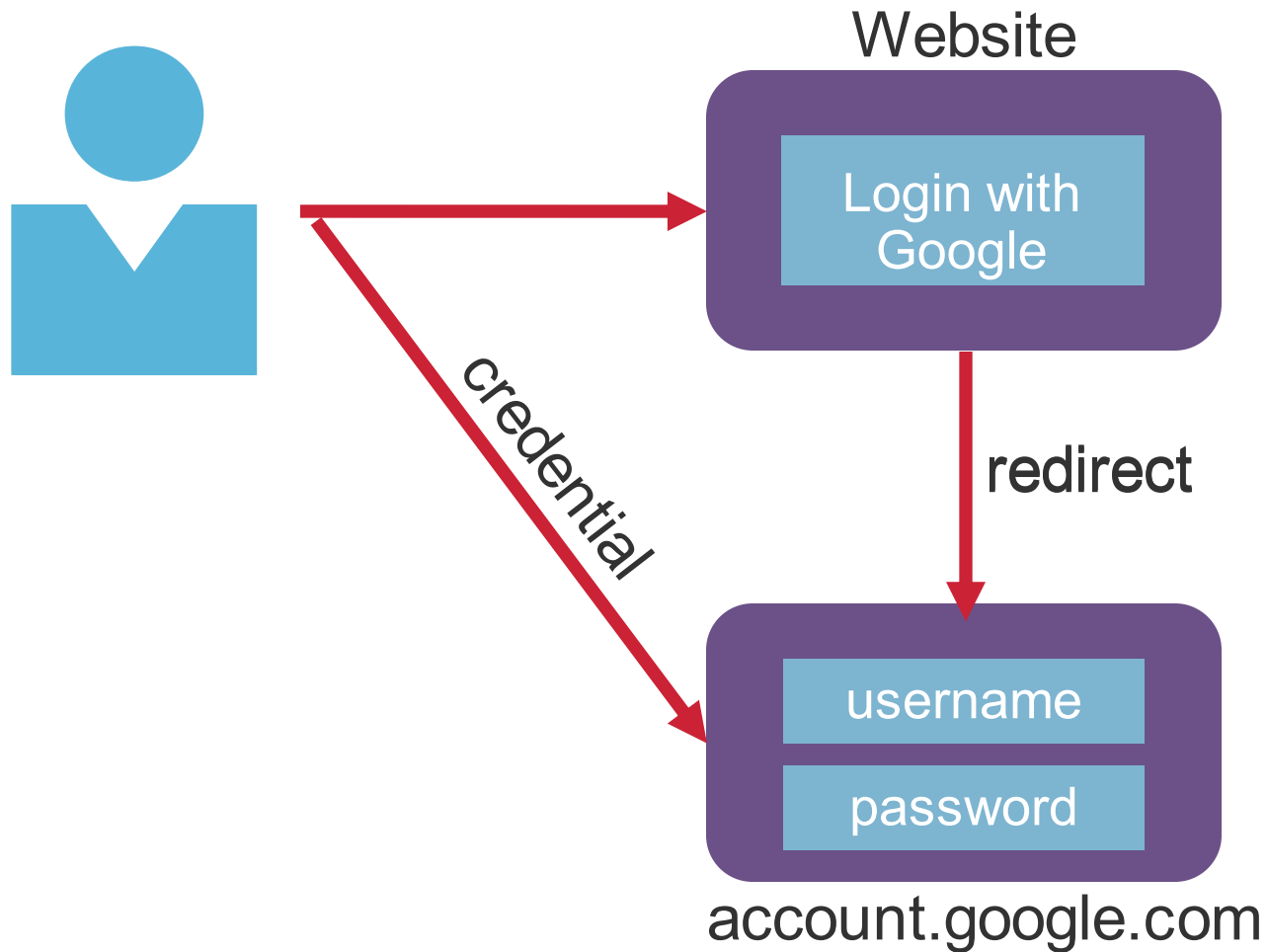
 Windows Live Hotmail

Find Friends

 Other Email Service

Find Friends

The delegated authorization with OAuth2.0



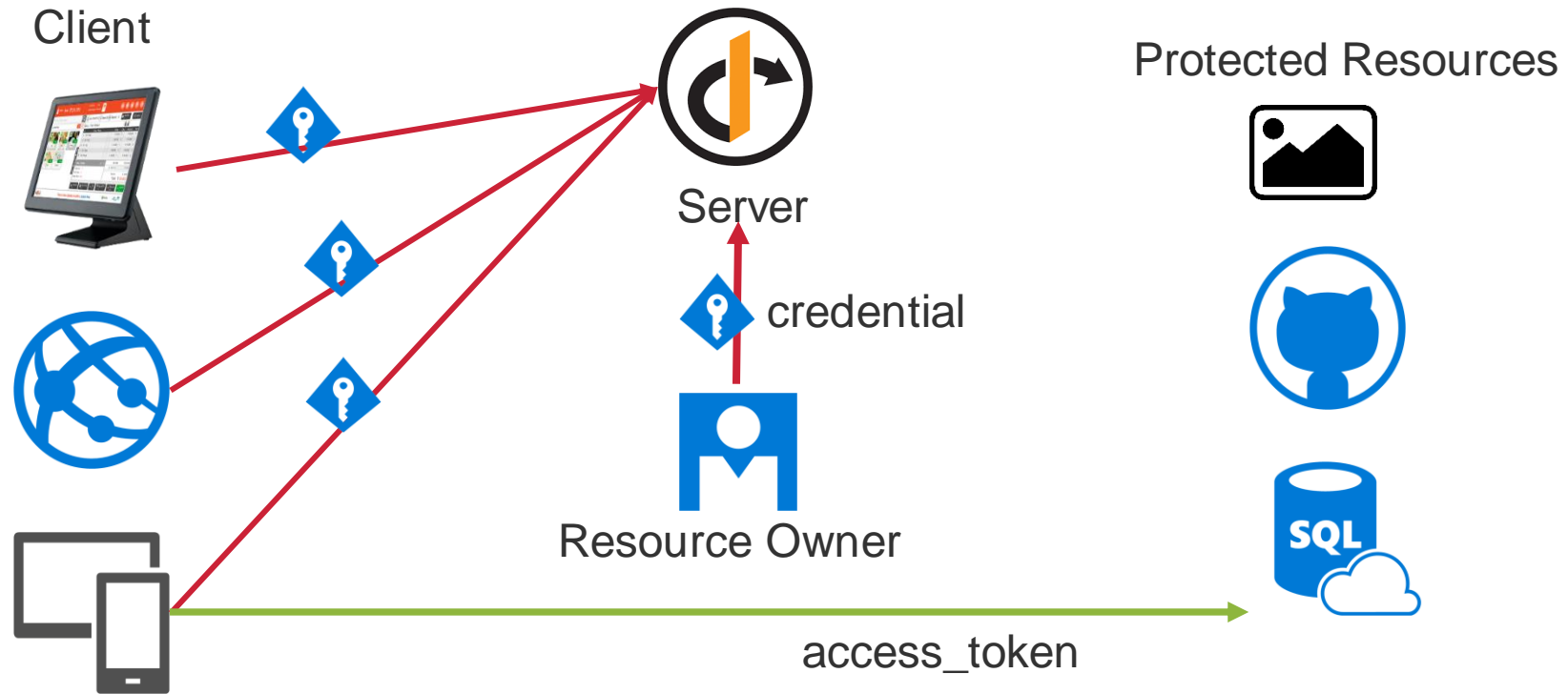


OAuth 2.0

Terminology

- Client: HTTP client capable of making OAuth-authenticated requests
- Server: An HTTP server capable of accepting OAuth-authenticated requests
- Protected resource: An access-restricted resource that can be obtained from the server using an OAuth-authenticated request
- Resource owner: User
- Credentials: Credentials are a pair of a unique identifier and a matching shared secret.
- Token: A unique identifier issued by the server and used by the client to associate authenticated requests

Factors



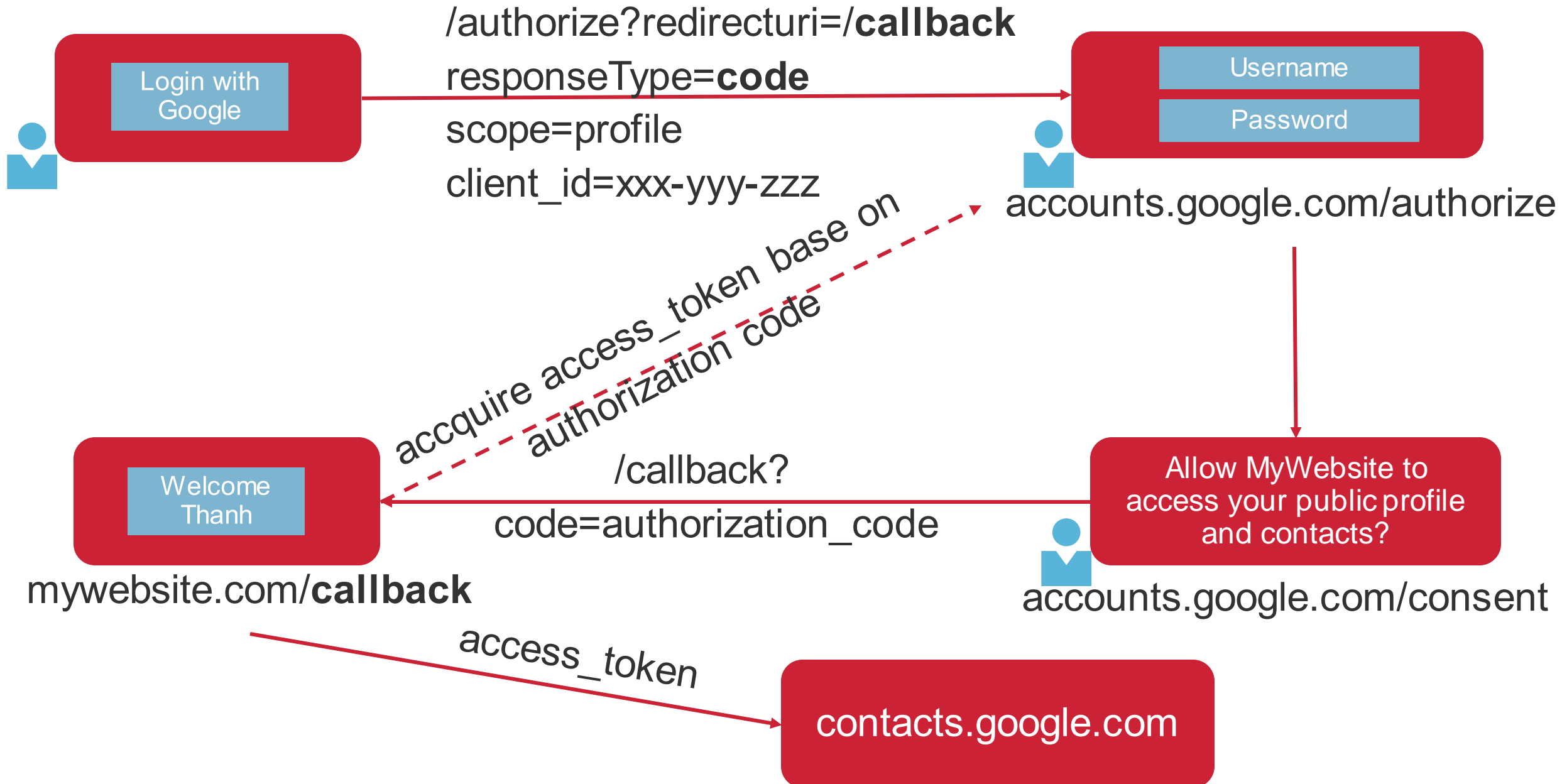
Grant Type

Grant type	Usage
Authorization code	MVC application that required user interaction.
Implicit	Single Page Application (SPA) like Angular, ReactJs.
Resource owner password	Use resource owner's username and password. Make the legacy system compatible with new system.
Client credential	Server to server communication.
Device Code	Non-browser authentication base

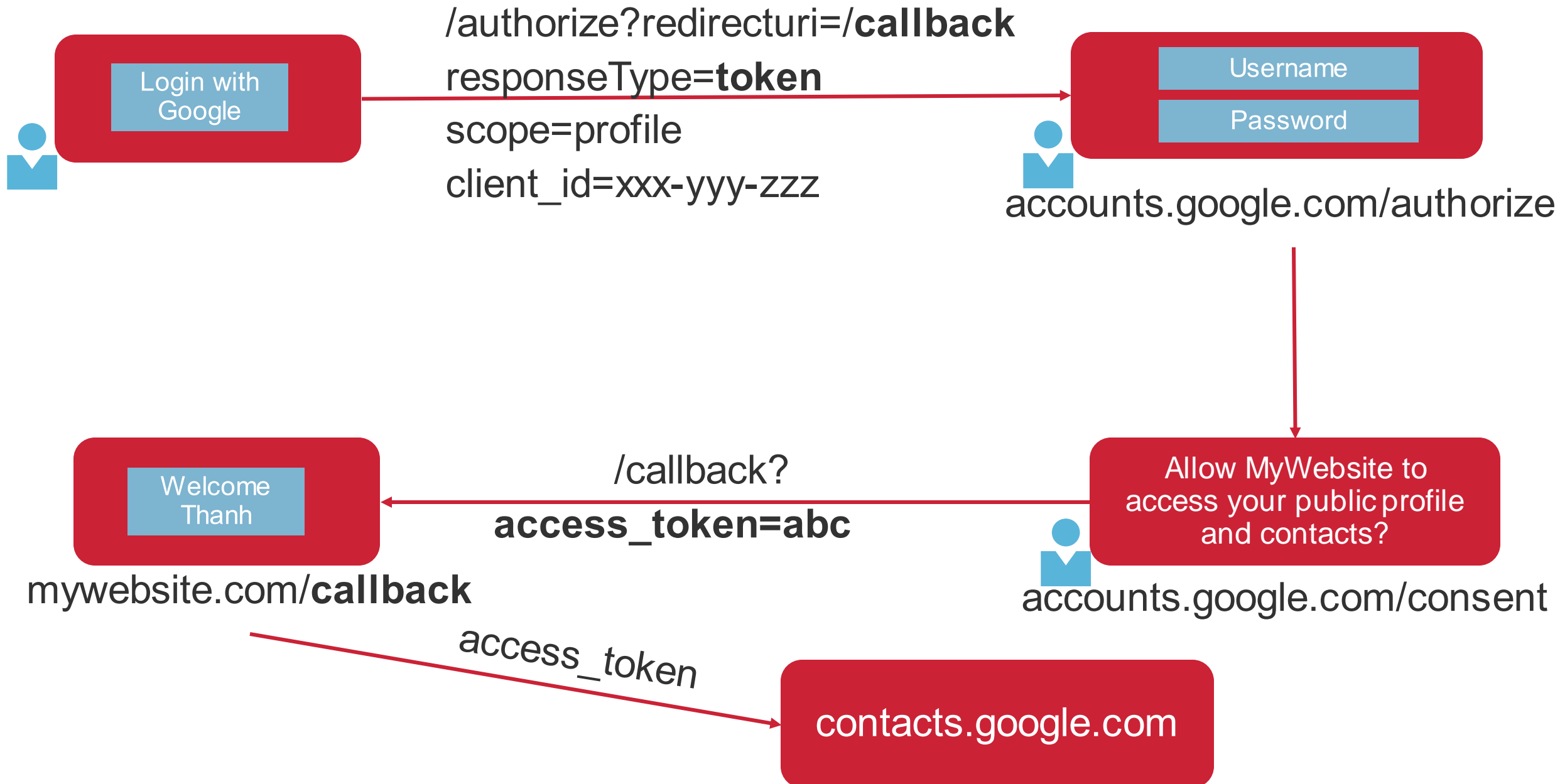
Channel

Type	Description
Front Channel	Single Page Application (SPA) like Angular, ReactJs.
Back Channel	Hosted by server like IIS, Tomcat. ASP.NET core MVC

Authorization code flow



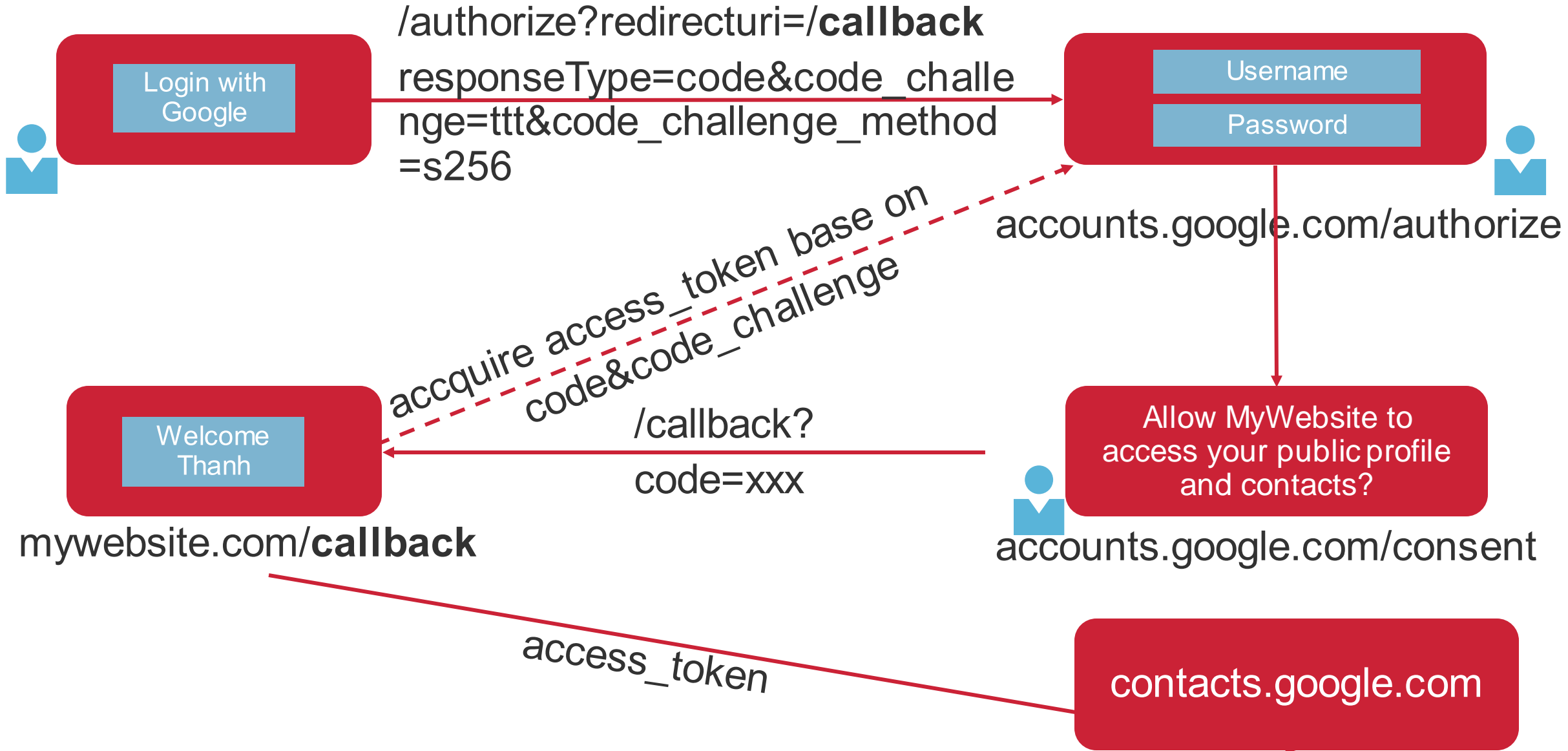
Implicit flow



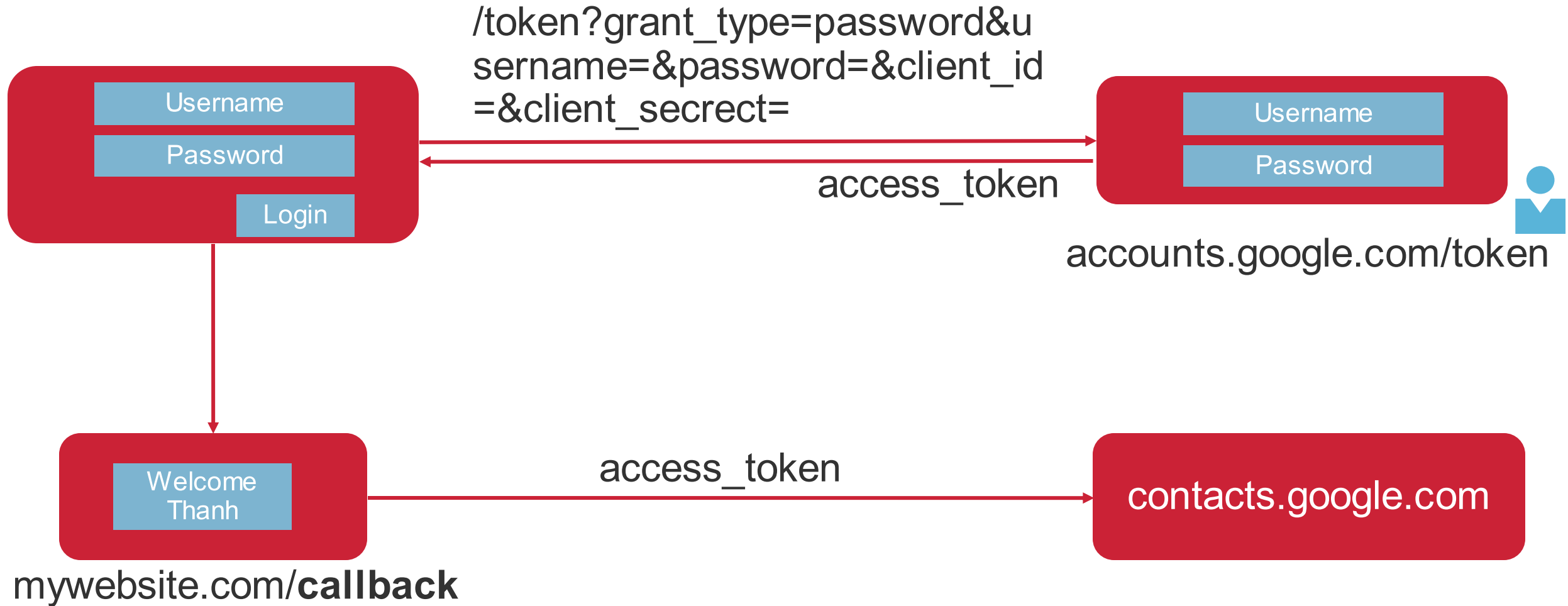
You should never use implicit flow again

- Token send directly in the browser.
- Leaking tokens is a big security risk.
- In November of 2018, new guidance was released that effectively deprecated this flow.
- It turns out there's an extension to the Authorization Code flow that's been in use for some time with Mobile and Native apps. That's Proof Key for Code Exchange or PKCE (pronounced "pixie").

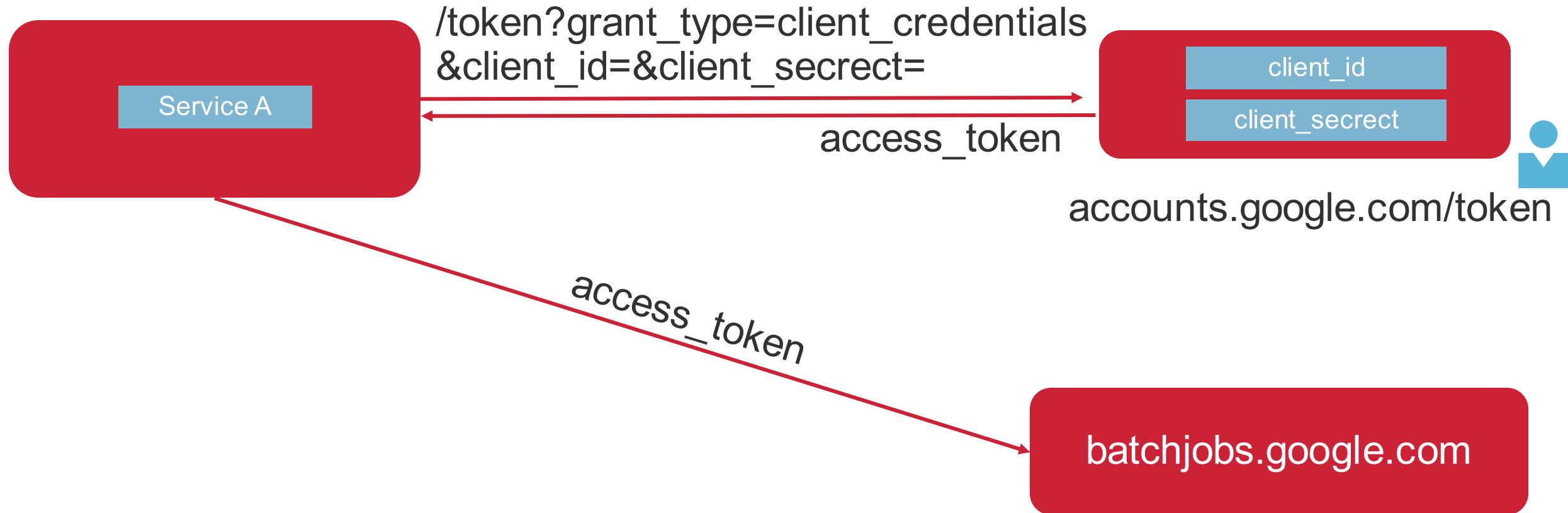
PKCE



Resource Owner Password

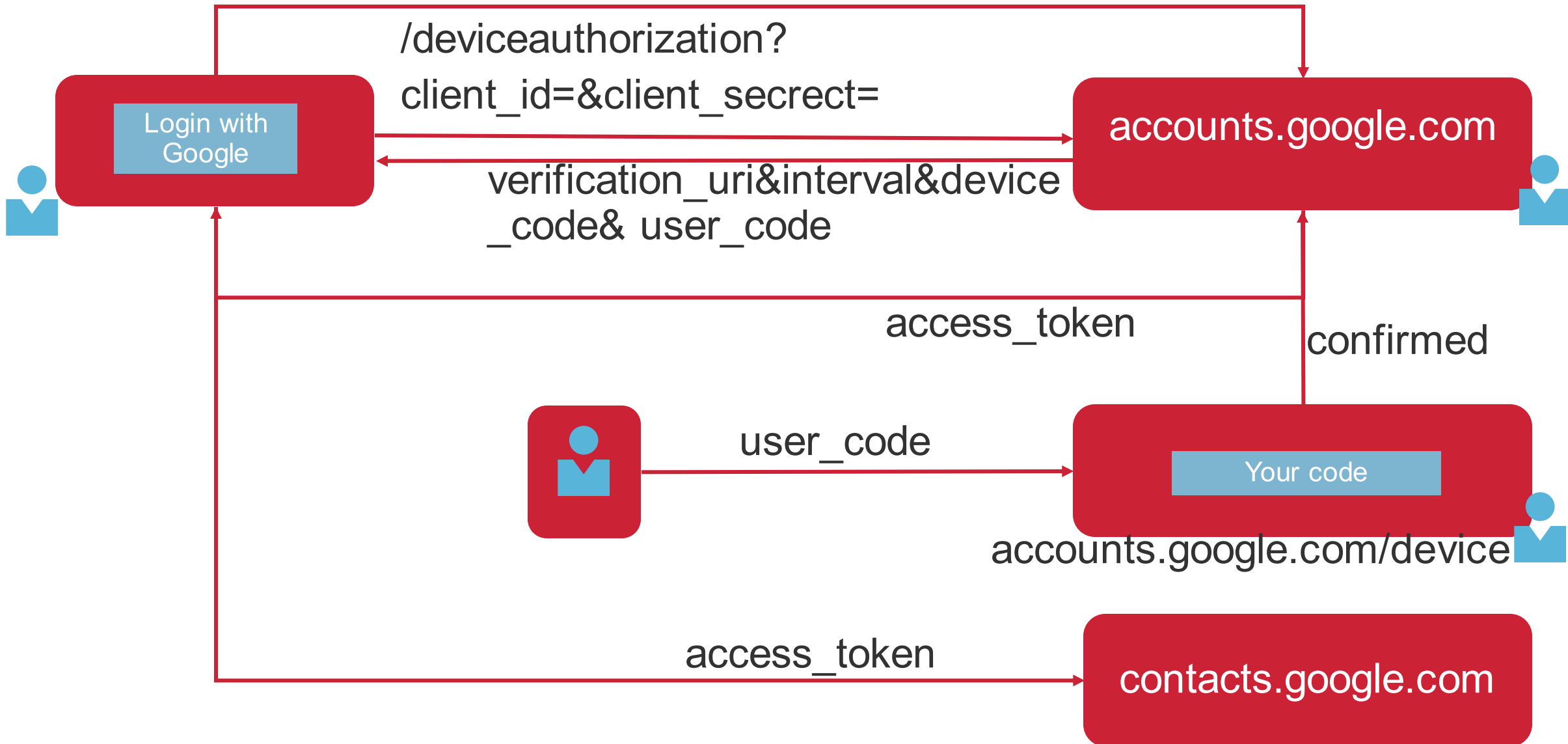


Client Credentials



Device Code

pooling each {{interval}}



Problems

- No standard way to get the user's information
- Every implementation is a little different
- No common set of scopes



OpenId Connect

OpenId Connect

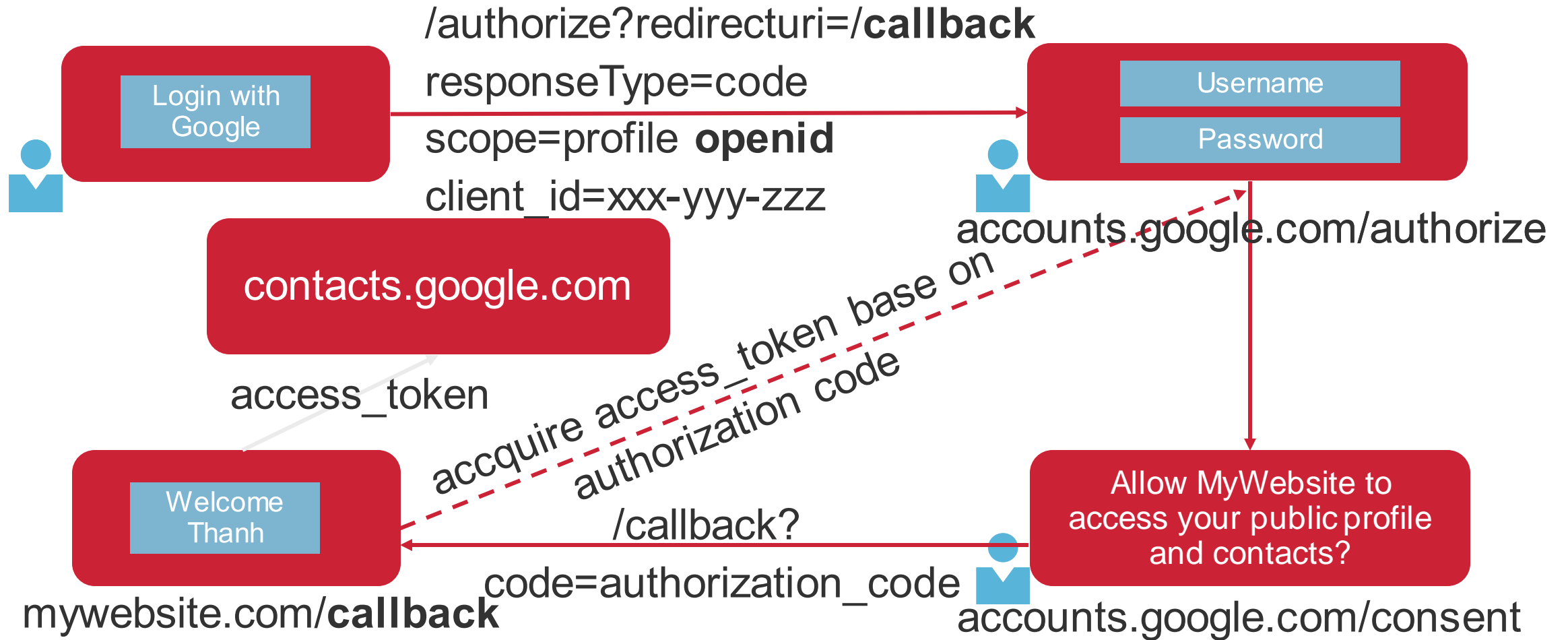
- ID token
- UserInfo endpoint for getting more user information
- Standard set of scopes
- Standardized implementation

OpenId Connect

OAuth2.0

HTTPS

Authorization code flow



OAuth <3 OpenID Connect

OAuth2.0	OpenId Connect
Granting access to your API	Logging the user in
Getting access to user data in other systems (Authorization)	Making your accounts available in other systems (Authentication)



Show me!

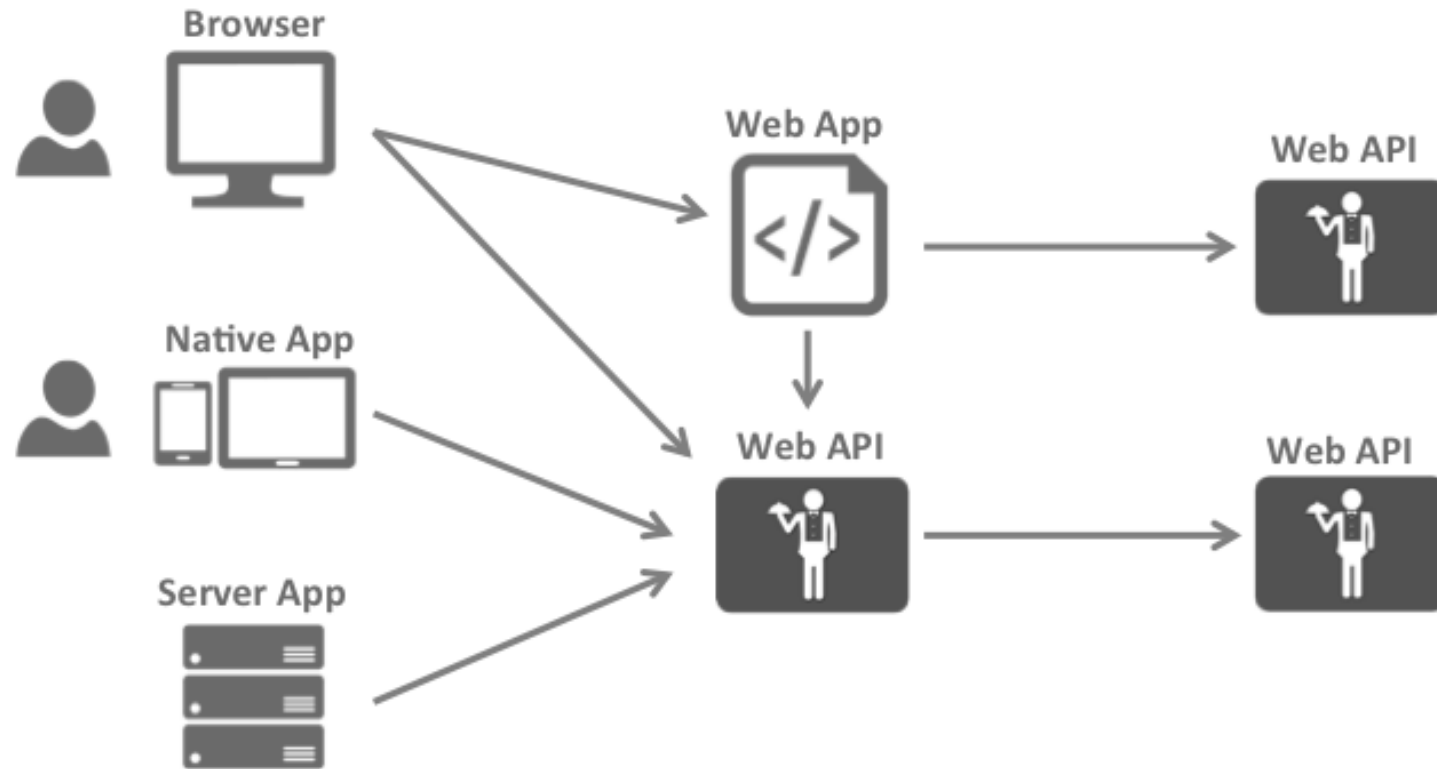


IdentityServer4

Features

- Authentication as a Service
- Single Sign-on / Sign-out
- Access Control for APIs
- Federation Gateway
- Focus on Customization

The Big Picture



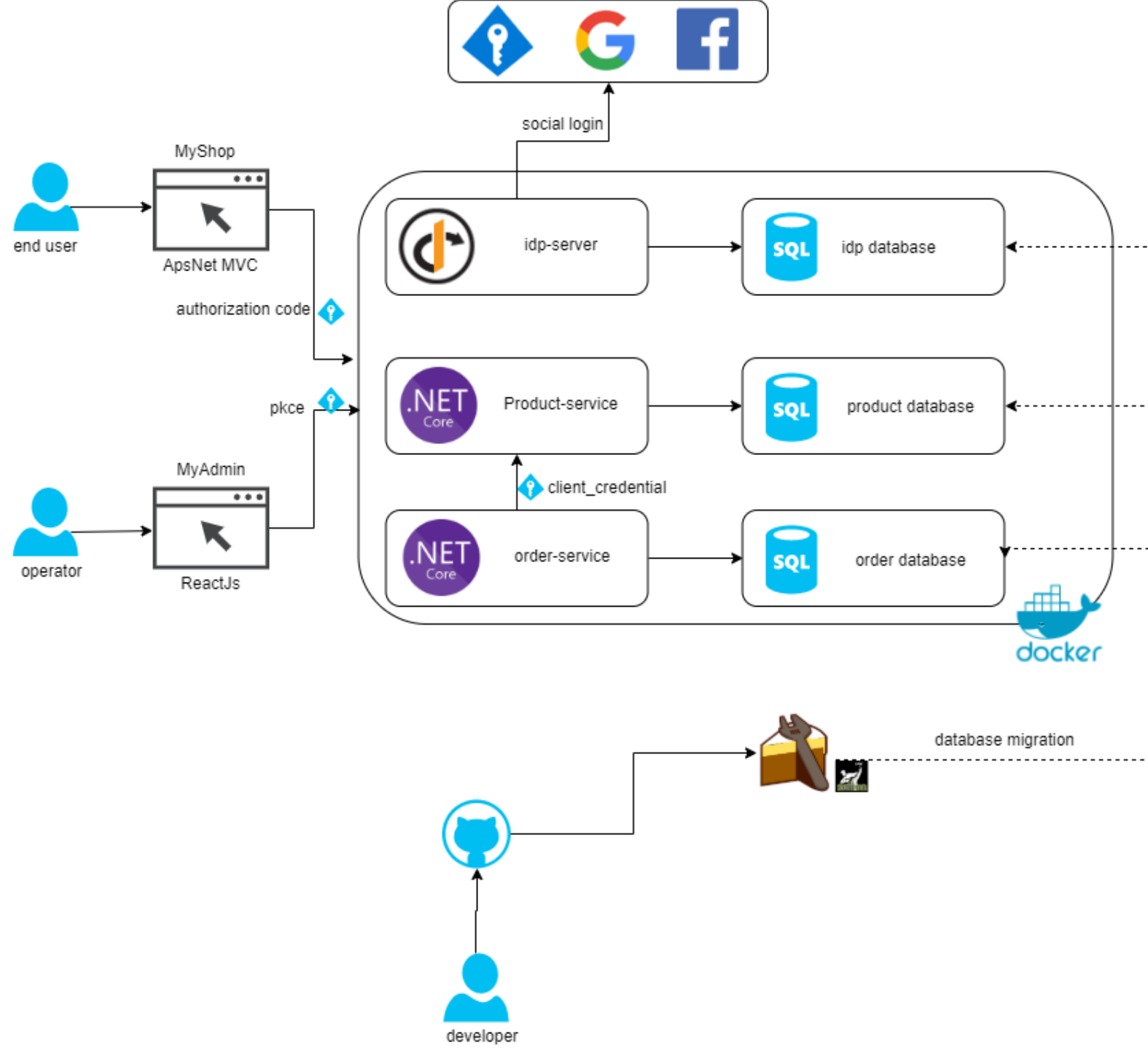
Endpoints (.well-known/openid-configuration)

Address	Description
/jwks	signature and public key
/authorize	to request tokens or authorization codes via the browser
/token	used to programmatically request tokens
/userinfo	retrieve identity information about a user
/endsession	trigger single sign-out
/checksession	check token lifetime
/revocation	revoking access tokens and refresh token
/deviceauthorization	request device and user codes

ApiResource & Client

- ApiResource: a resource in your system that you want to protect
- Client: use to access our new API

DEMO





Q&A

References

- <https://tools.ietf.org/html/rfc2617>
- <https://tools.ietf.org/html/rfc7616>
- <https://tools.ietf.org/html/rfc7617>
- <https://tools.ietf.org/html/rfc6749>
- <https://tools.ietf.org/html/rfc5849>
- <https://tools.ietf.org/html/rfc6750>
- https://simple.wikipedia.org/wiki/Chosen-plaintext_attack
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication>
- <https://tools.ietf.org/html/rfc7519>
- https://docs.oracle.com/cd/E39820_01/doc.11121/gateway_docs/content/part_oauth.html
- http://openid.net/specs/openid-connect-core-1_0.html



THANK YOU

www.nashtechglobal.com

