All About Auth

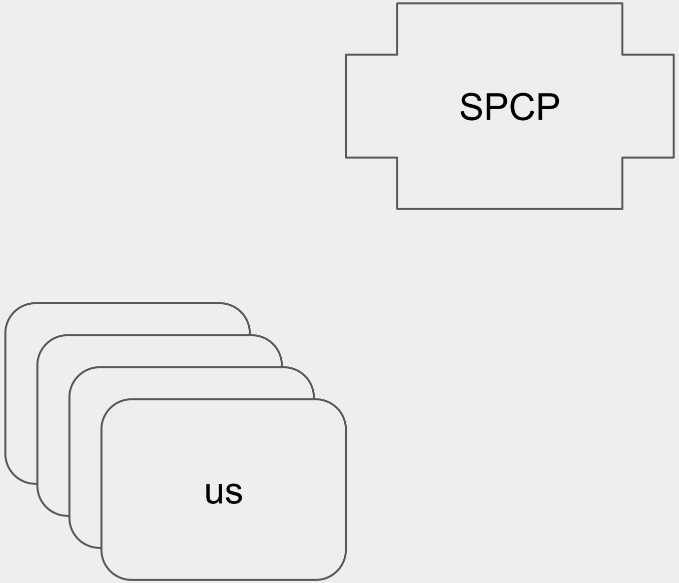
Tokens, Sessions and Redirects

Samantha Wong,
ACE Software Engineering
Meetup - 26 Feb 2021

Or, What We Learned Building an Auth Common Service in GoBusiness

Why We Started This Journey

Necessity is the Mother of Production



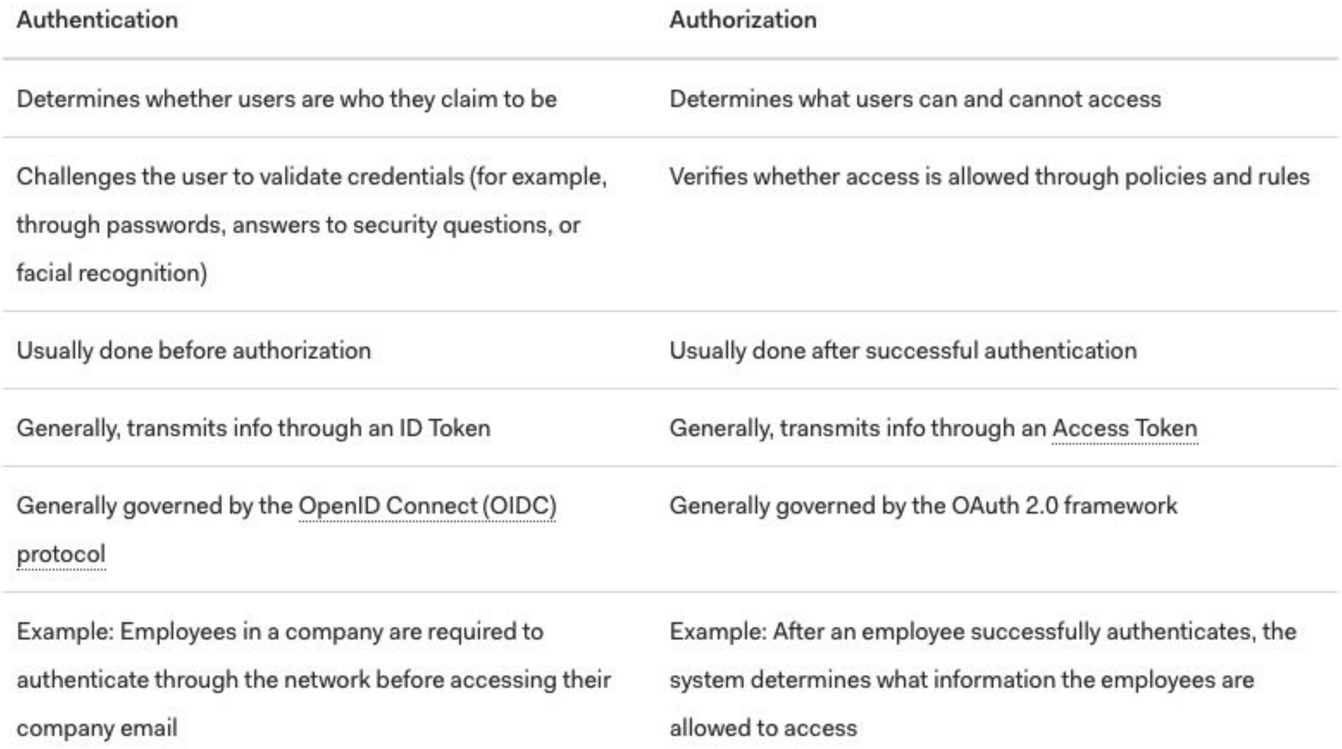
Auth(entication) V. Auth(orization)

Entity access

Verifies entity identity

Authentication vs Authorization

According to auth0



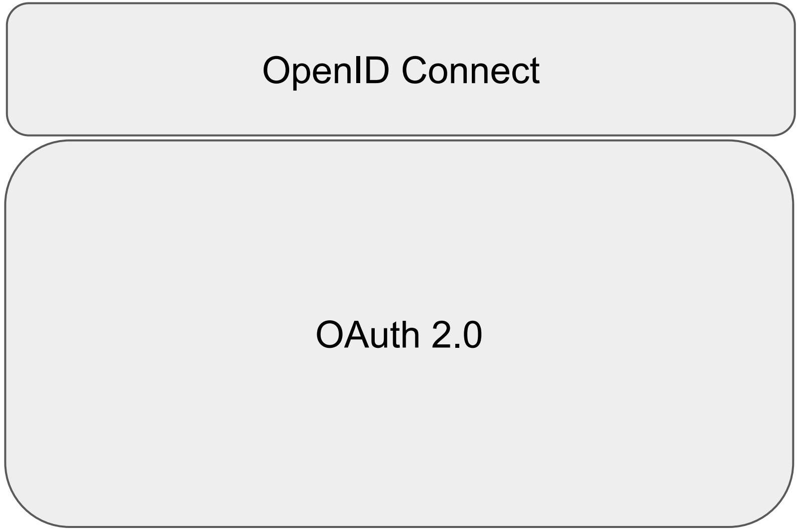
Authentication	Authorization
Determines whether users are who they claim to be	Determines what users can and cannot access
Challenges the user to validate credentials (for example, through passwords, answers to security questions, or facial recognition)	Verifies whether access is allowed through policies and rules
Usually done before authorization	Usually done after successful authentication
Generally, transmits info through an ID Token	Generally, transmits info through an Access Token
Generally governed by the OpenID Connect (OIDC) protocol	Generally governed by the OAuth 2.0 framework
Example: Employees in a company are required to authenticate through the network before accessing their company email	Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access

Salt

Beef

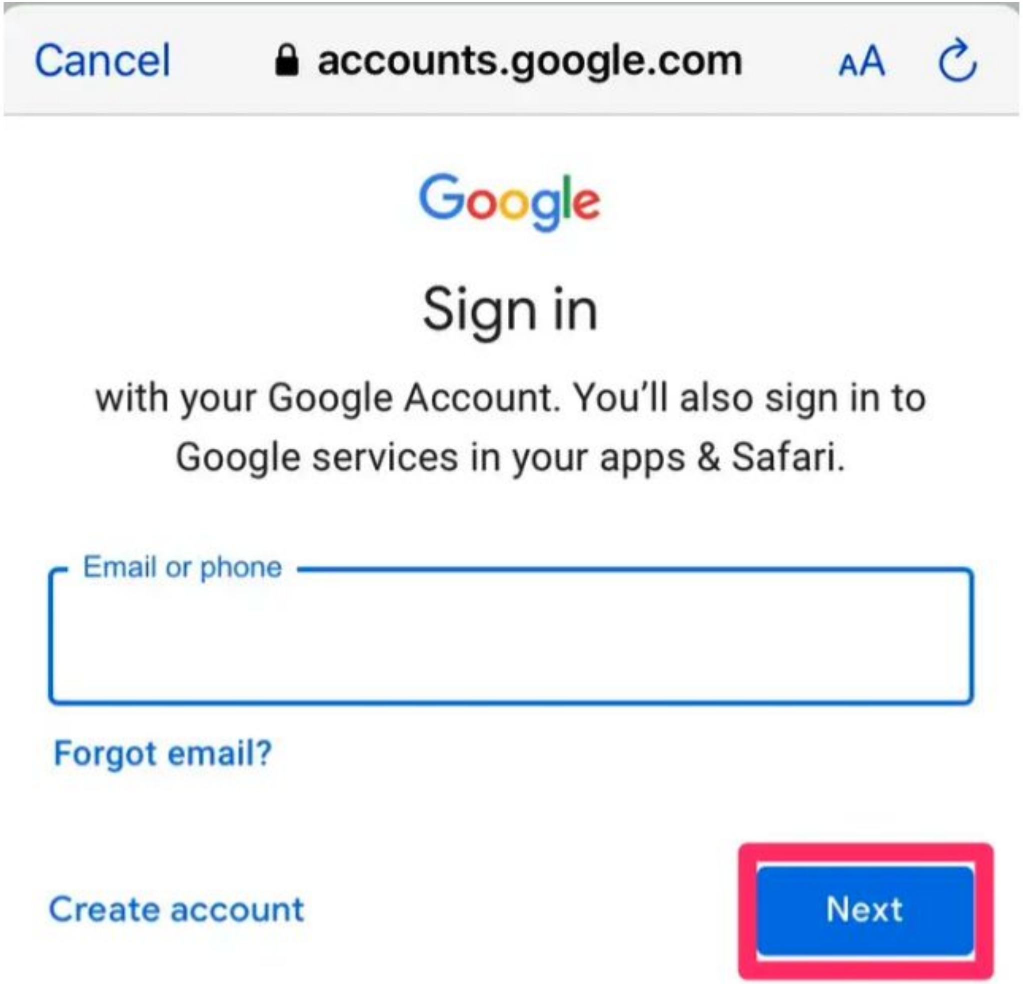
Source: https://auth0.com/docs/flows

OpenID Connect (OIDC) - OAuth



OpenID Connect

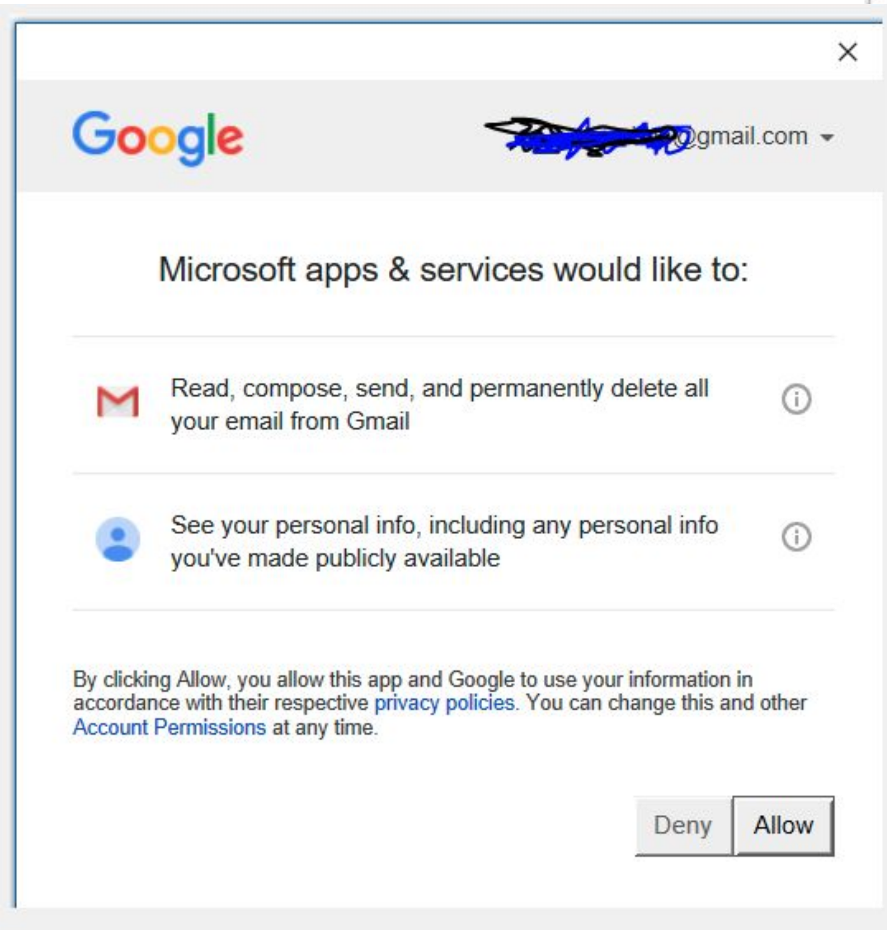
OAuth 2.0



Sign in

with your Google Account. You'll also sign in to Google services in your apps & Safari.

OIDC



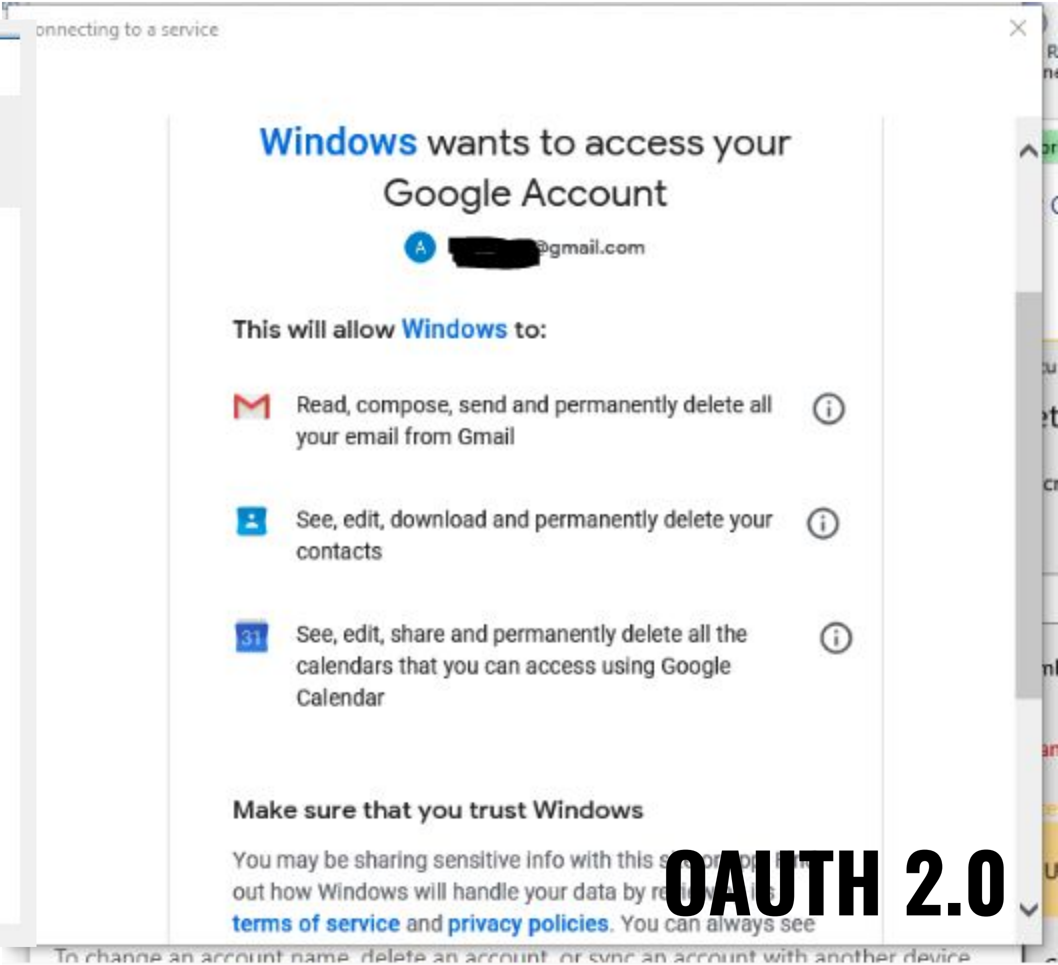
Google [redacted]@gmail.com

Microsoft apps & services would like to:

Read, compose, send, and permanently delete all your email from Gmail

See your personal info, including any personal info you've made publicly available

By clicking Allow, you allow this app and Google to use your information in accordance with their respective privacy policies. You can change this and other Account Permissions at any time.



onnecting to a service

Windows wants to access your Google Account

[redacted]@gmail.com

This will allow Windows to:

Read, compose, send and permanently delete all your email from Gmail

See, edit, download and permanently delete your contacts

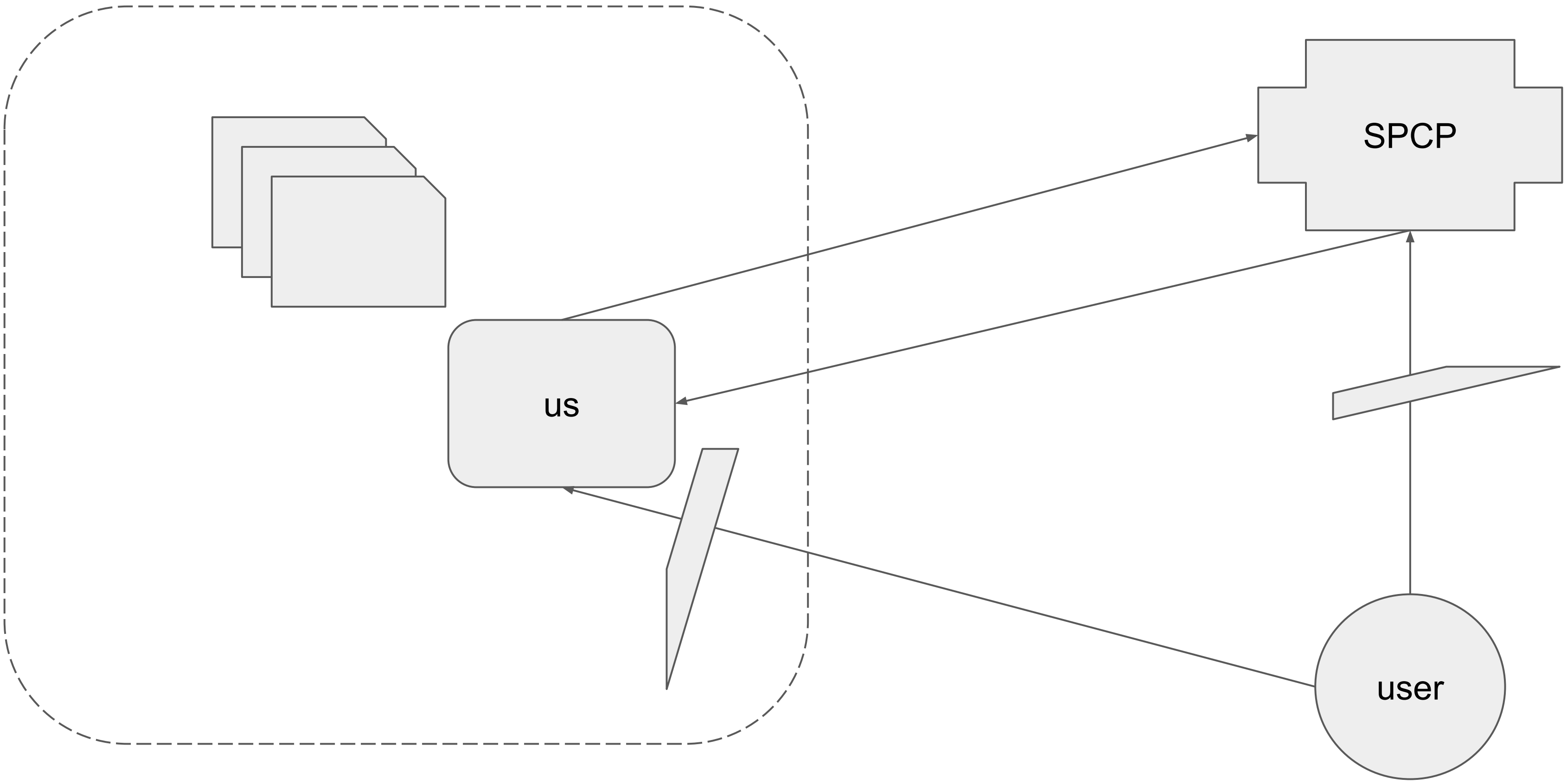
See, edit, share and permanently delete all the calendars that you can access using Google Calendar

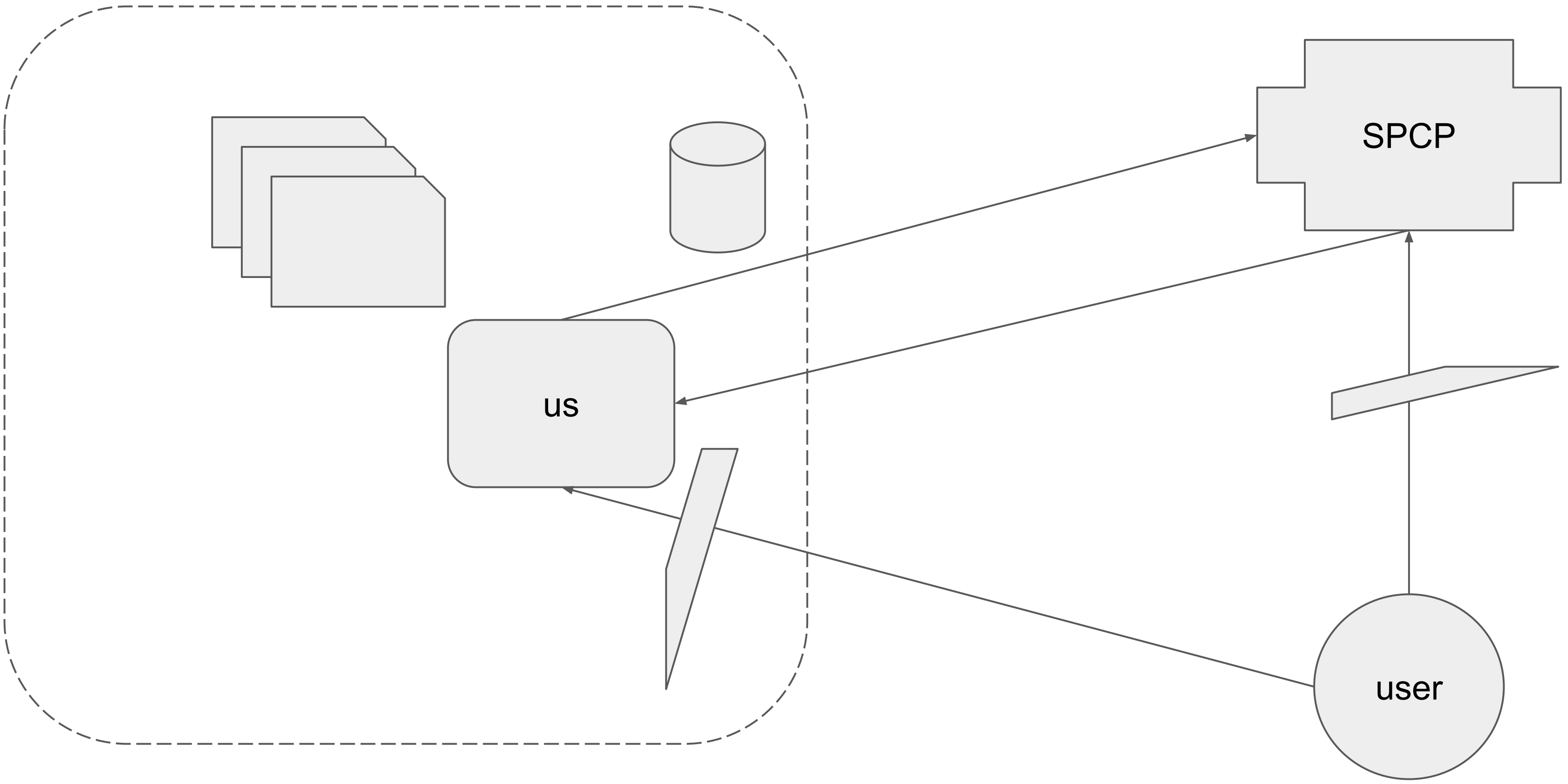
Make sure that you trust Windows

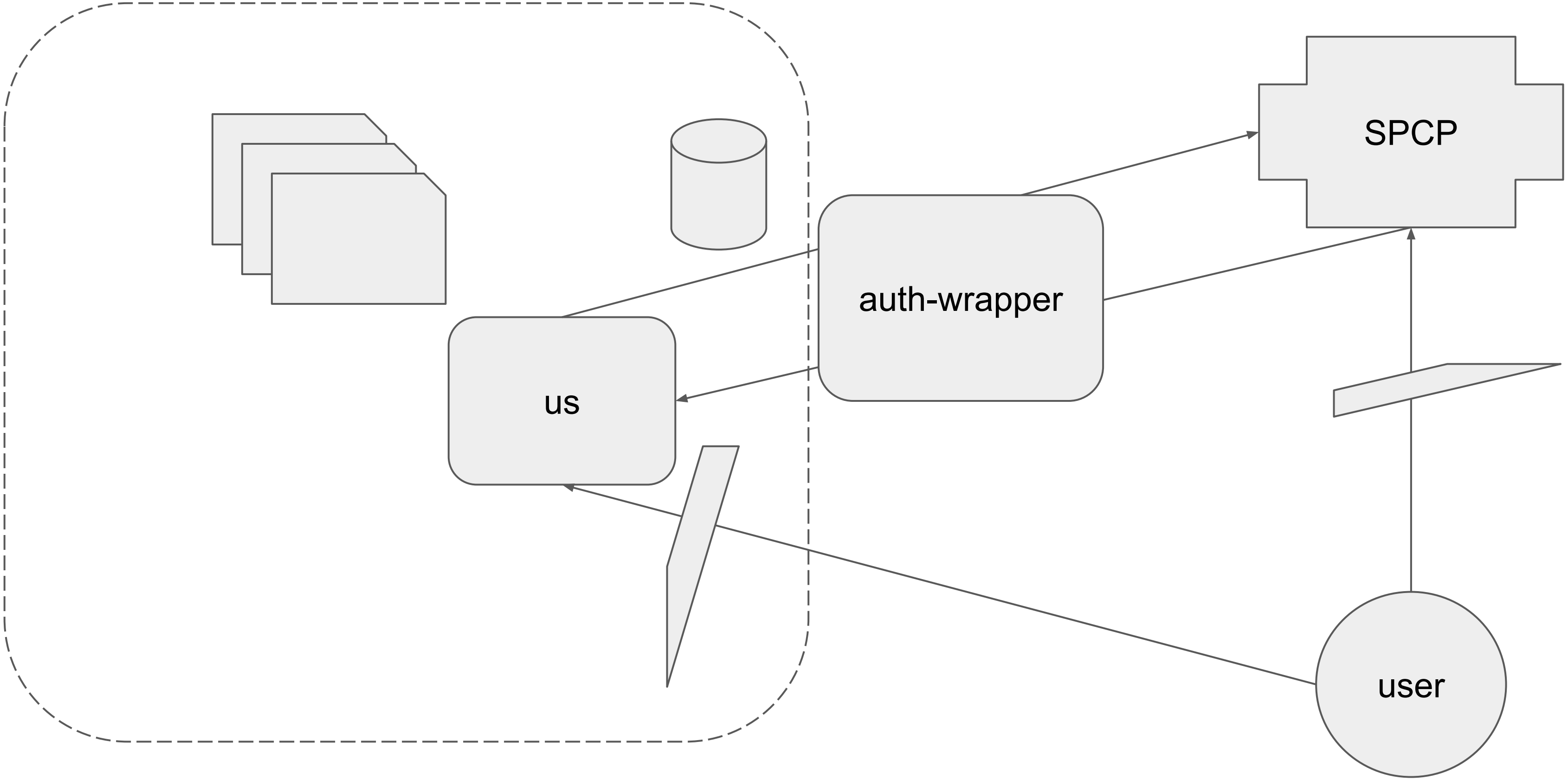
You may be sharing sensitive info with this s
out how Windows will handle your data by re
terms of service and privacy policies. You can always see

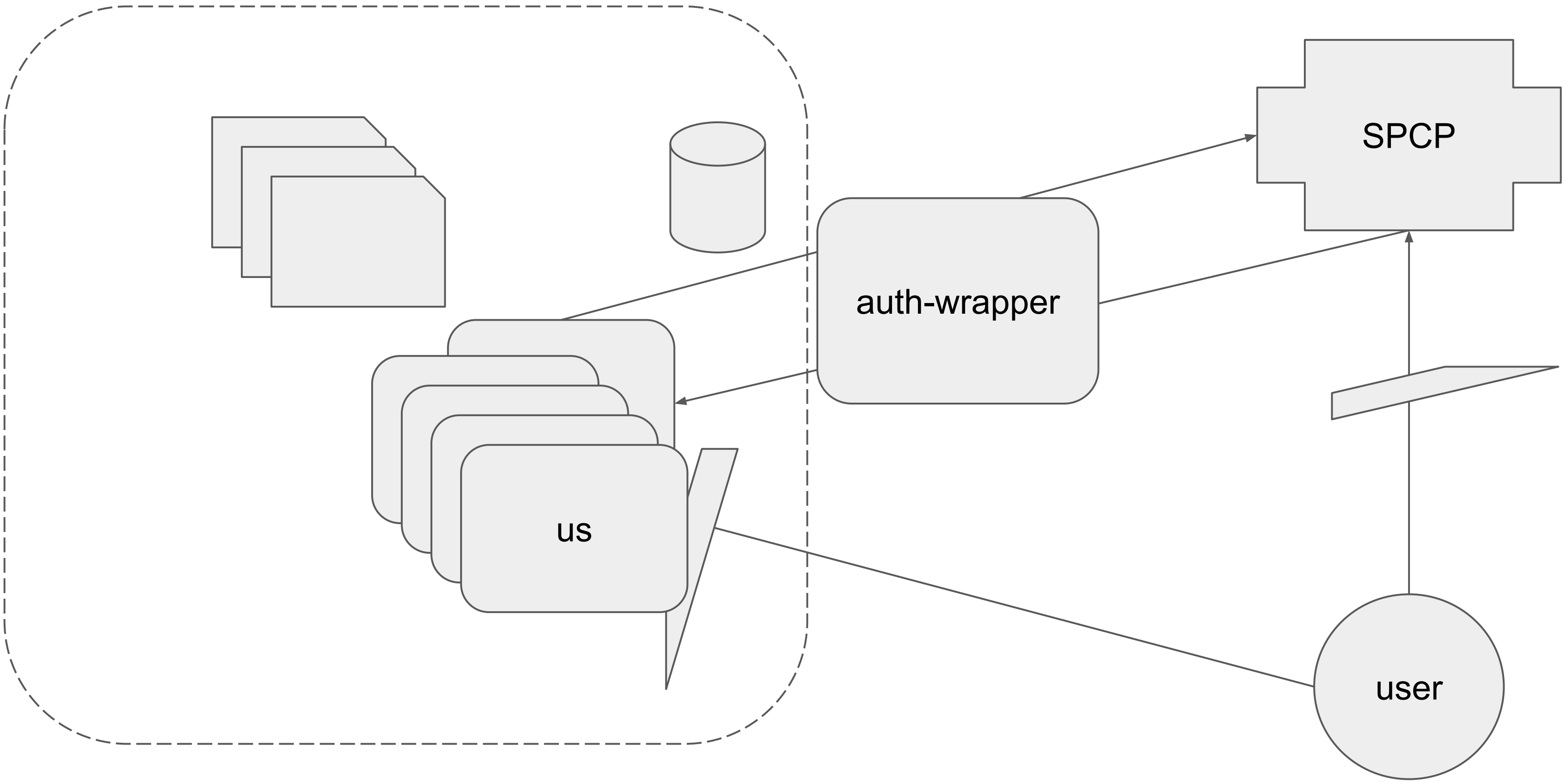
To change an account name, delete an account, or sync an account with another device

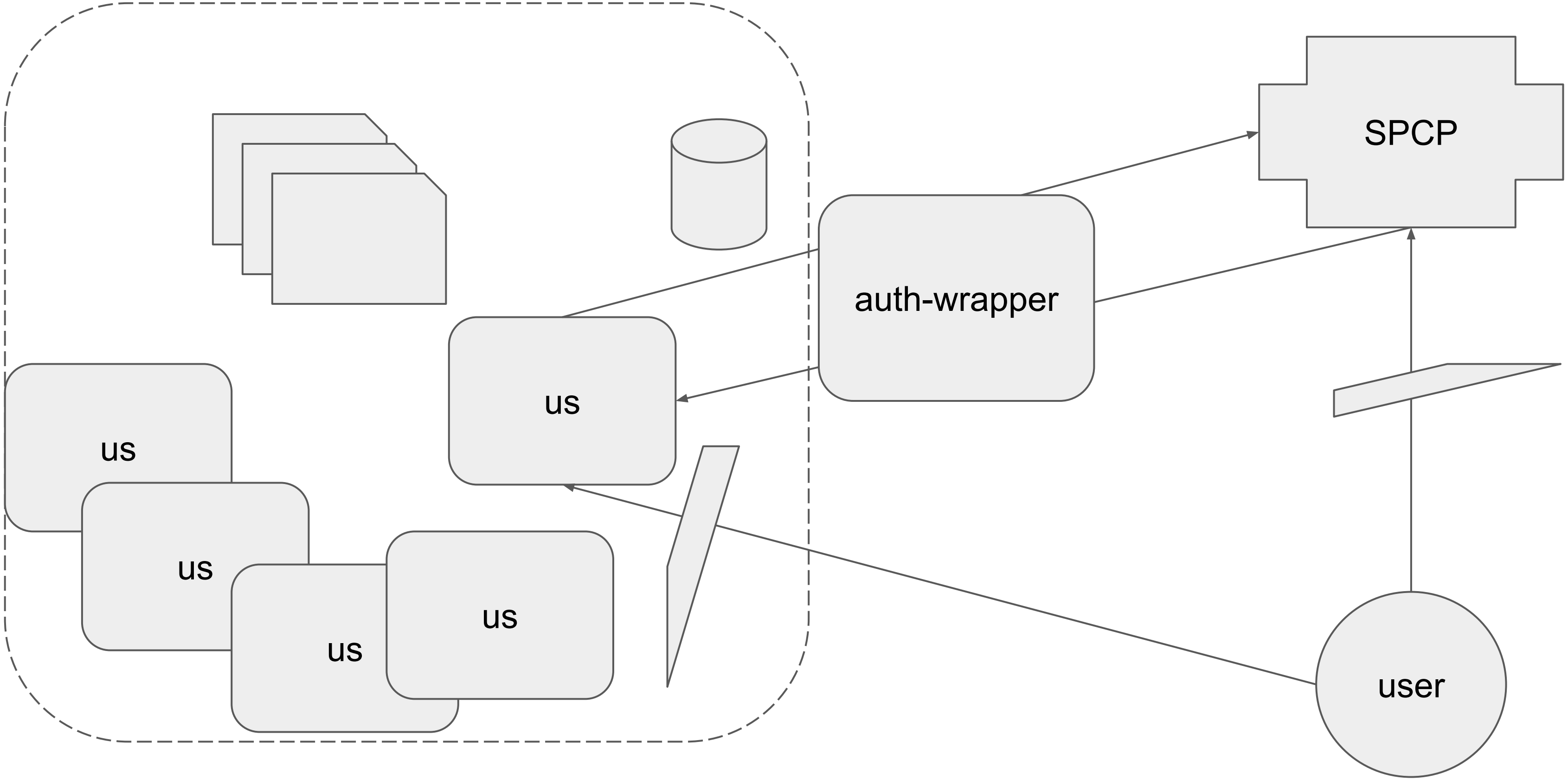
OAUTH 2.0

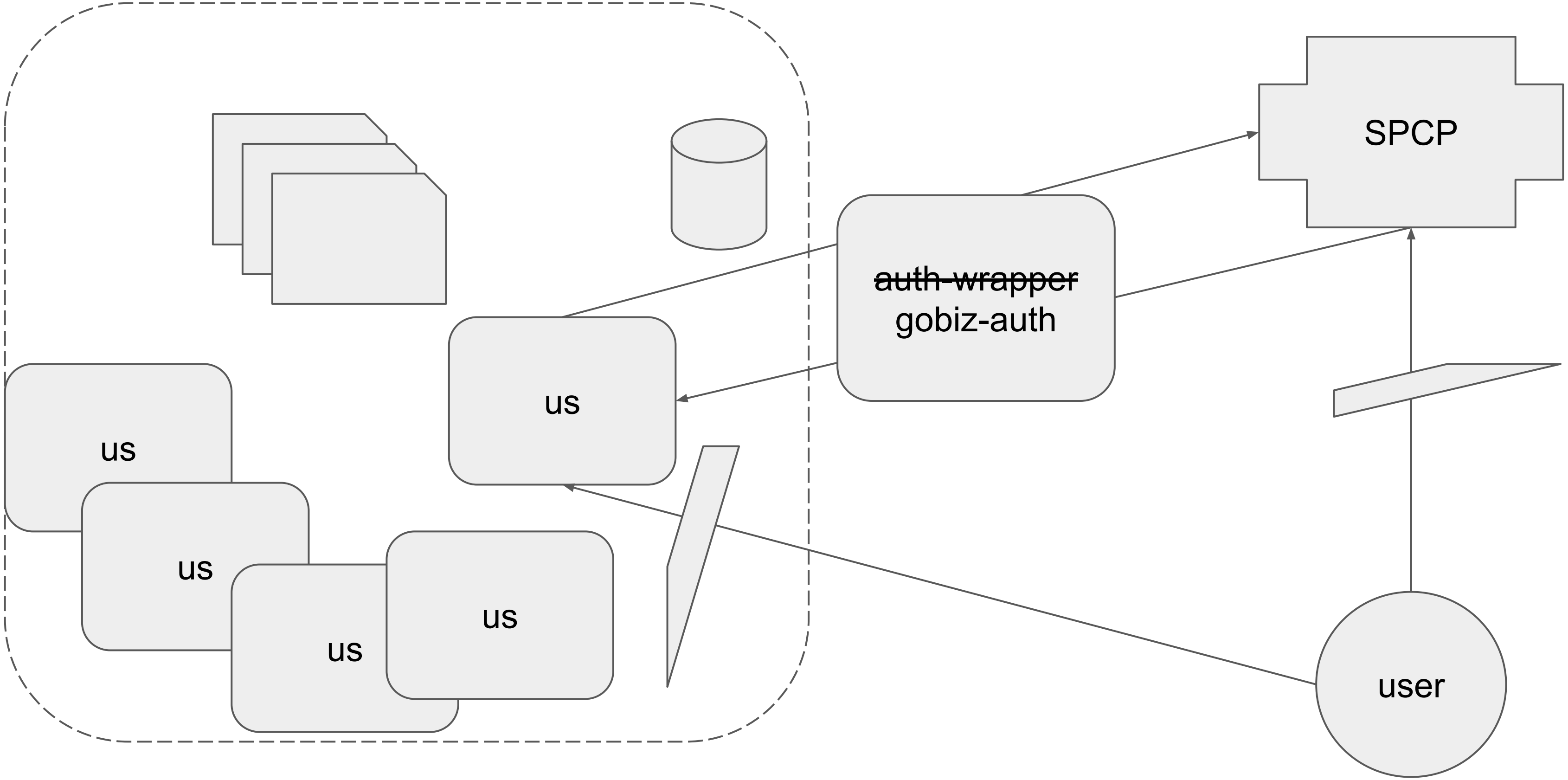

SPCP
us
user


SPCP
us
user


SPCP
auth-wrapper
us
user


SPCP
auth-wrapper
us
user


SPCP
auth-wrapper
us
us
us
us
us
user

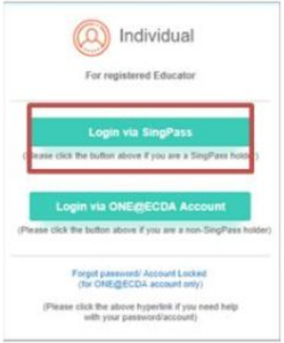

SPCP
~~auth-wrapper~~
gobiz-auth
us
us
us
us
us
user

But wait, doesn’t SPCP have SSO?

The below flow describes single sign on flow between different OIDC based digital services

End Users

User access digital service website



Individual

For registered Educator

Login via SingPass

(Please click the button above if you are a SingPass holder)

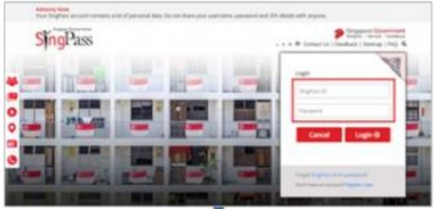
Login via ONE@ECDA Account

(Please click the button above if you are a non-SingPass holder)

Forgot password/ Account Locked
(for ONE@ECDA account only)

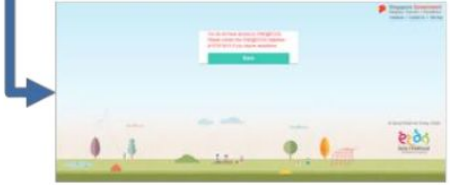
(Please click the above hyperlink if you need help with your password/account)

Redirected to SignPass Login Page

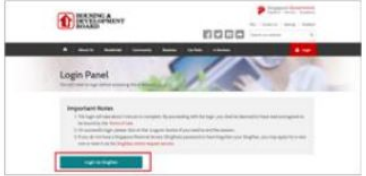


User enters credentials and click on Login Page

Landed to Digital Service Home page

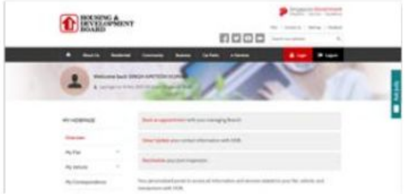


Access another digital service in same browser

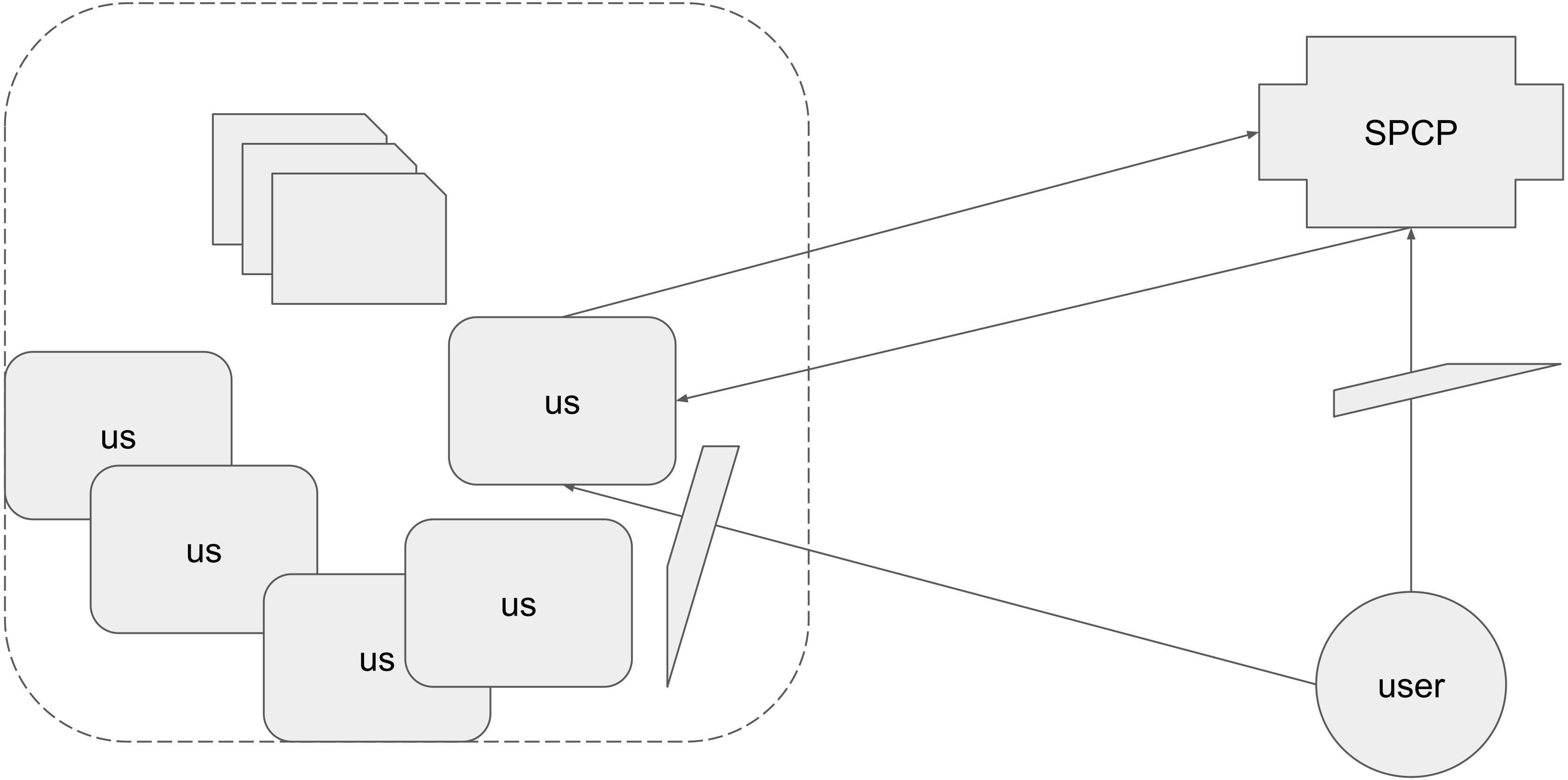


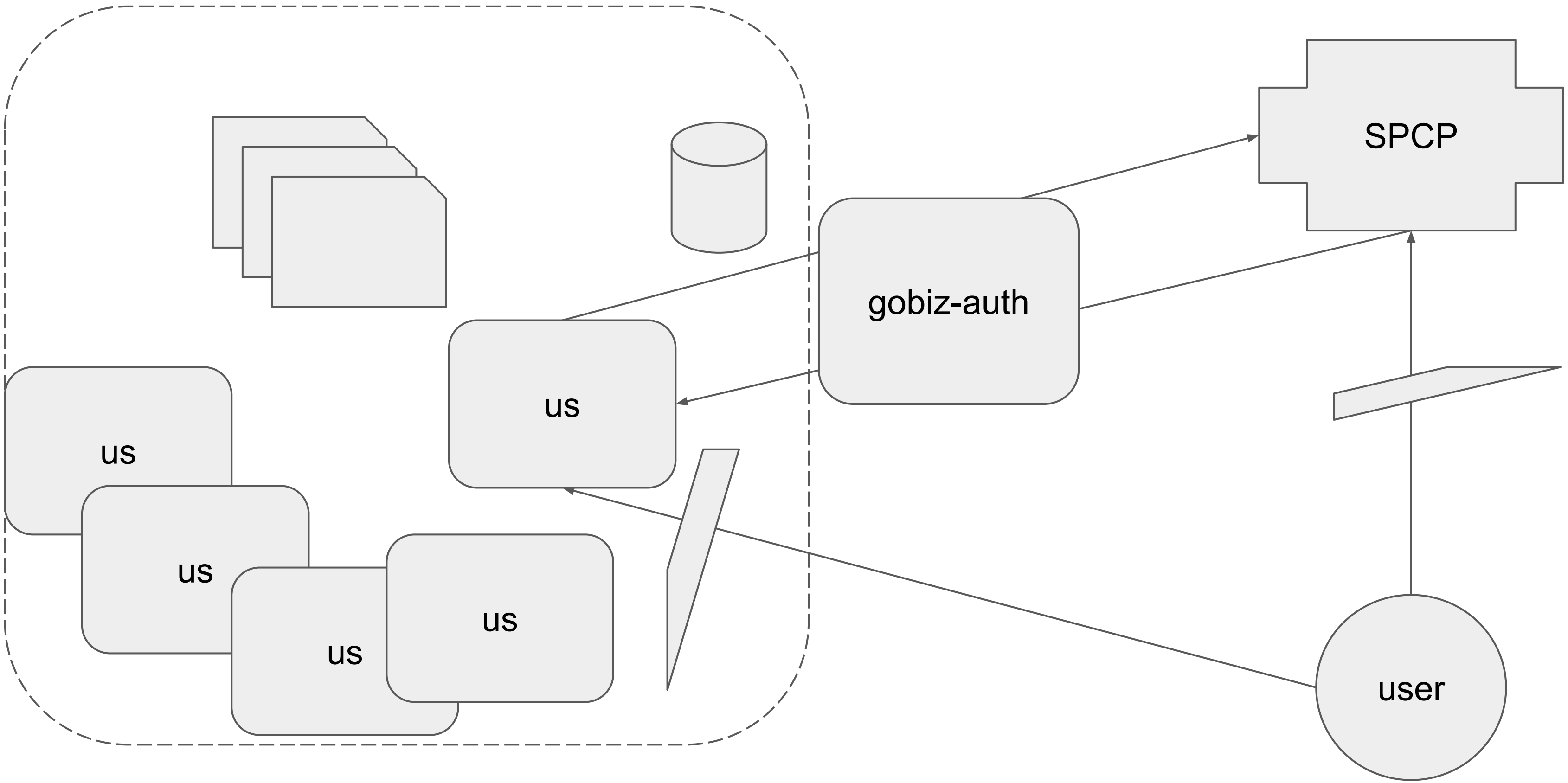
Clicks on Login with SingPass button

Landed to Digital Service Home page



Taken from SPCP OIDC Interface Specifications v1.5

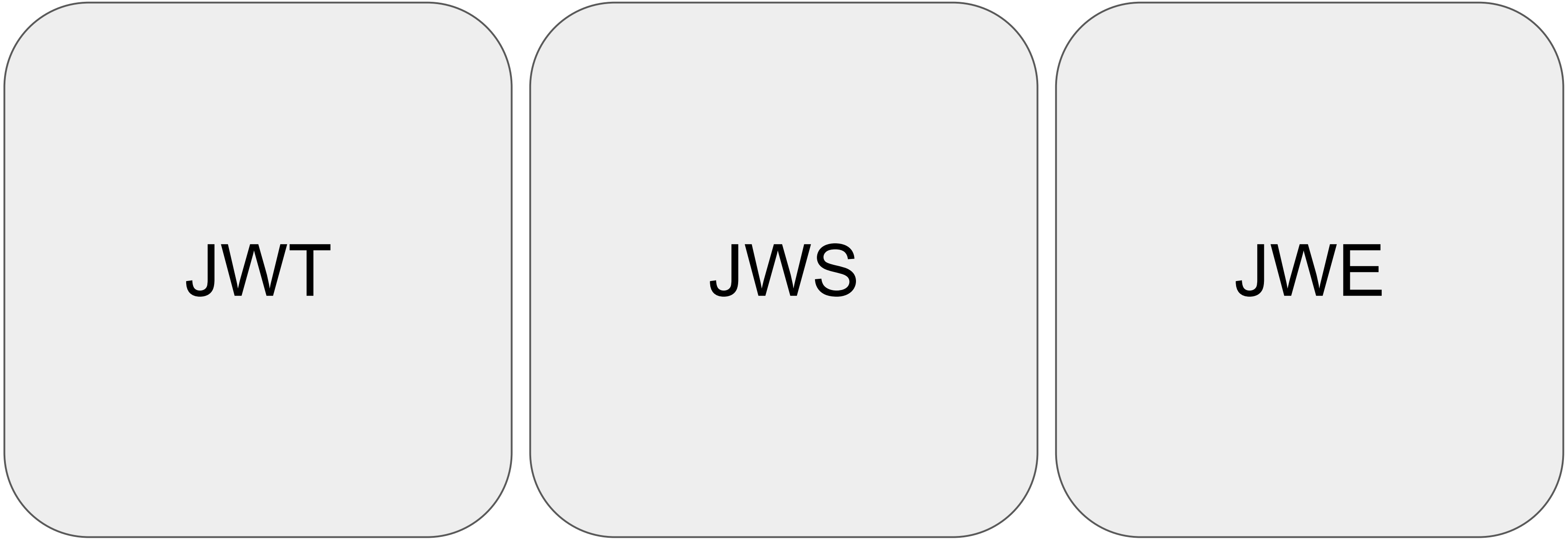

SPCP
us
us
us
us
us
user


SPCP
gobiz-auth
us
us
us
us
us
user

What’s in a Token

- Types of JWTs
- Why have a refresh and an access token and where to put them

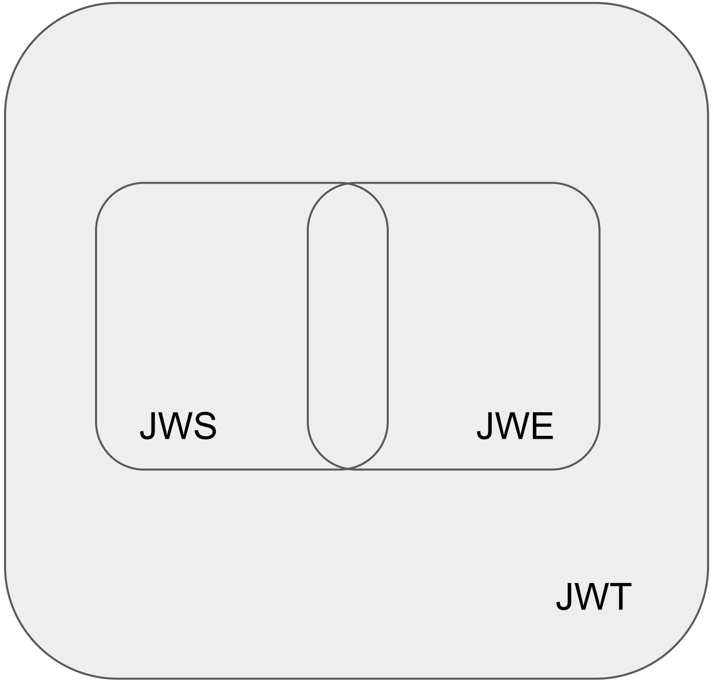
JWTs



JWT

JWS

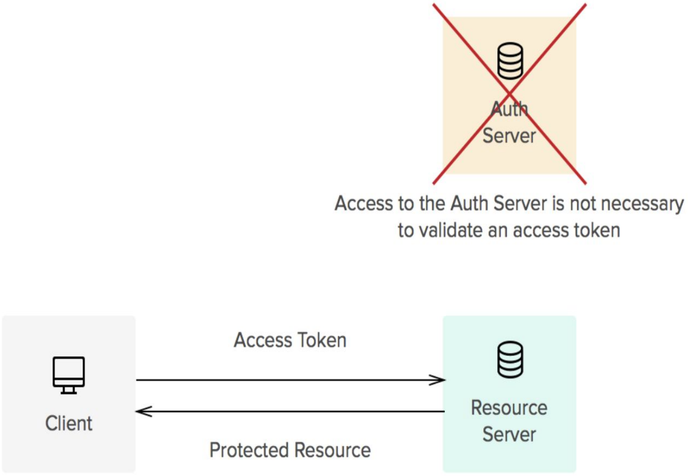
JWE

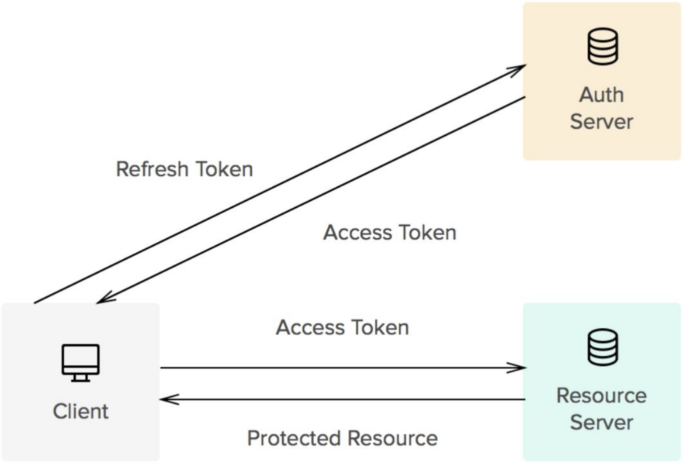

JWS
JWE
JWT

ID, Refresh and Access Tokens

- Short-lived
- About direct **access** to resources

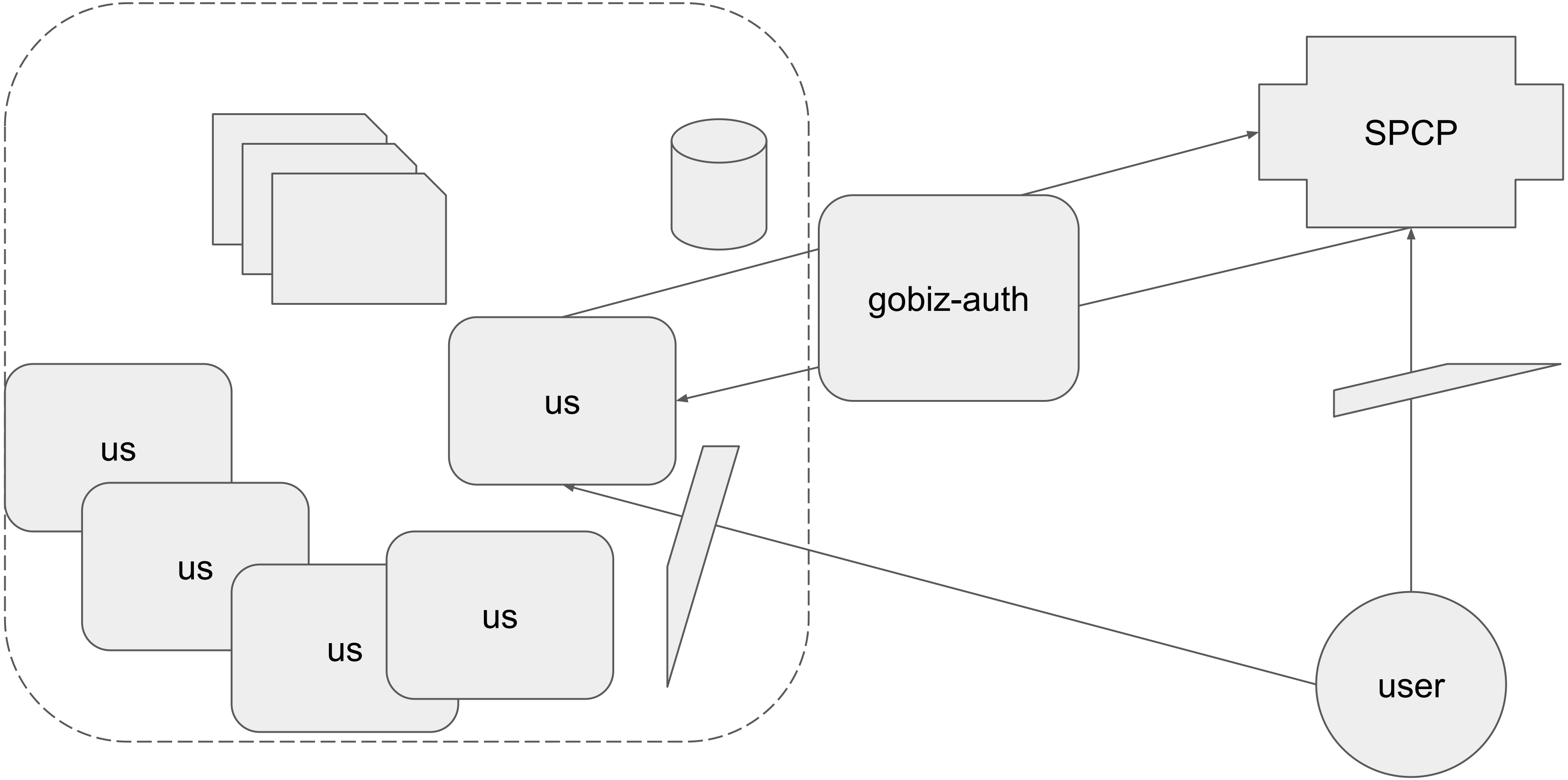
- Longer-lived
- Allows one to **refresh** access tokens

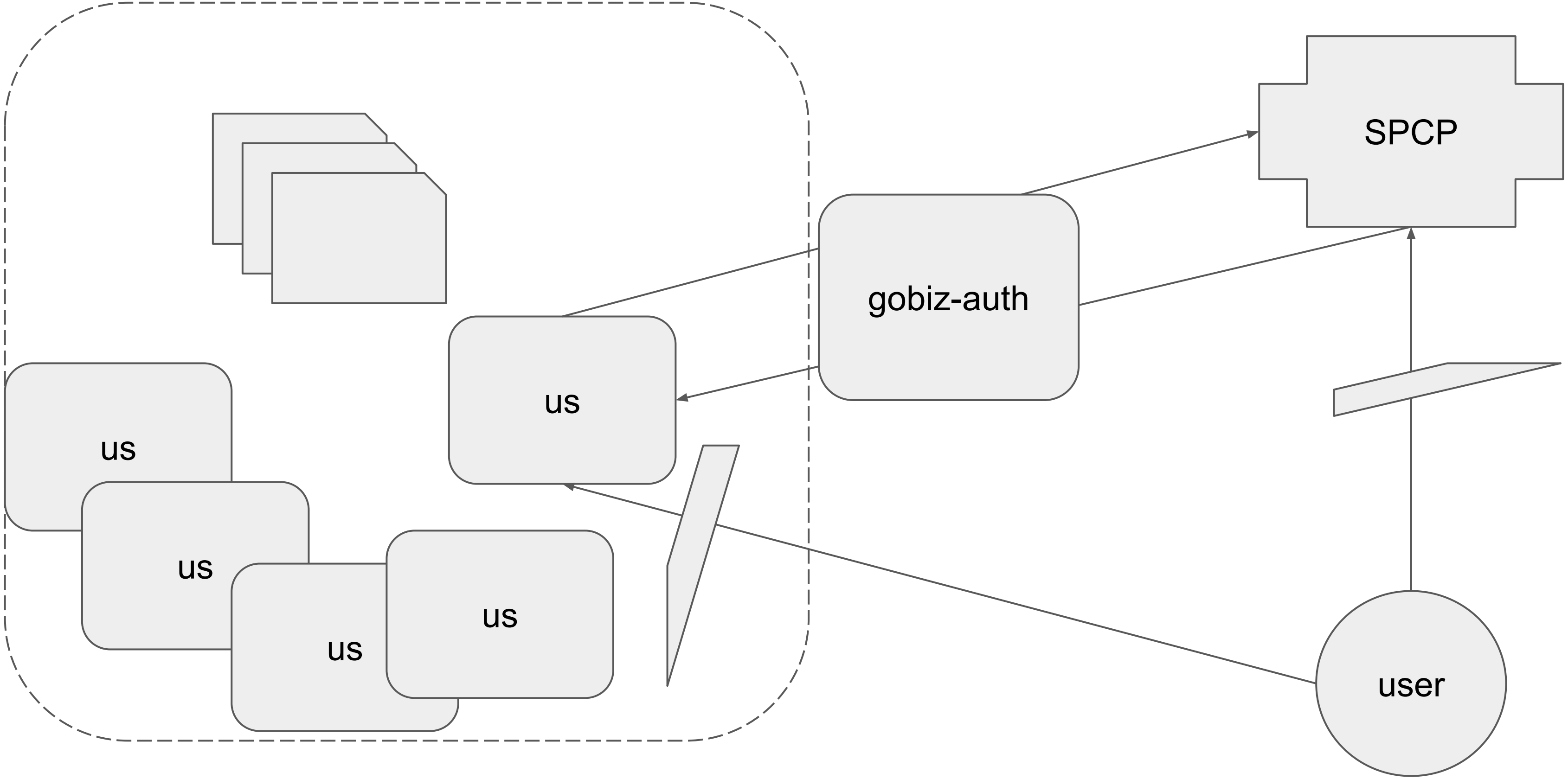

Auth Server
Access to the Auth Server is not necessary to validate an access token
Access Token
Client
Resource Server
Protected Resource



Source: https://auth0.com/blog/refresh-tokens-what-are-they-and-when-to-use-them/

Can we do without
some kind of
server-side storage?


SPCP
gobiz-auth
us
us
us
us
us
user

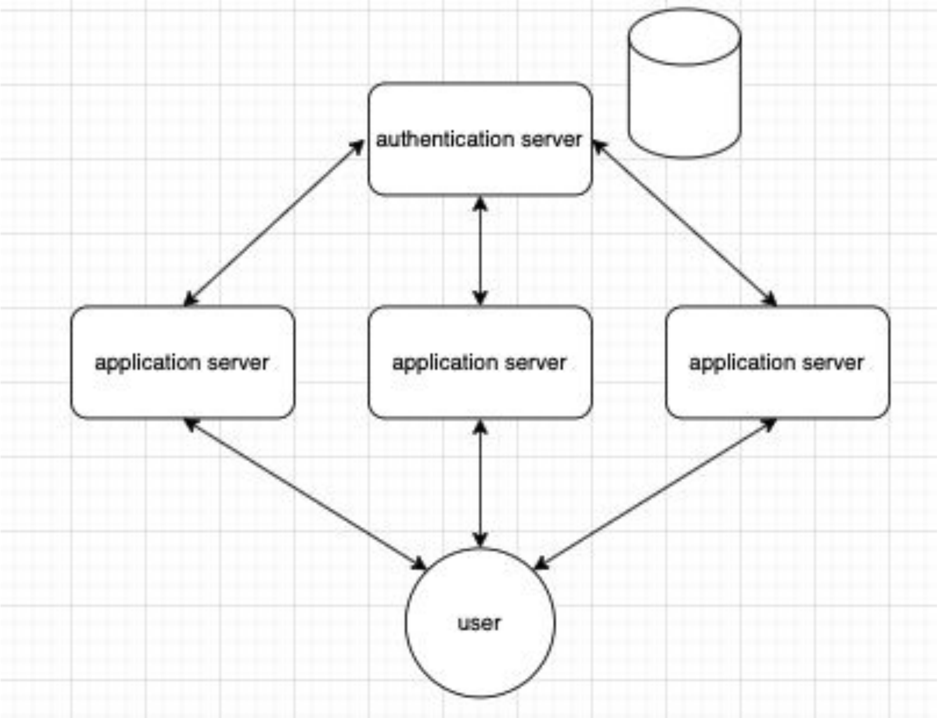

SPCP
gobiz-auth
us
us
us
us
us
user

No, we can’t log users out.

Eager Server Validation vs Offline Token Validation

Why one or the other? =

Supporting no concurrent users



Hypothetically,

/refresh: refreshes your access token

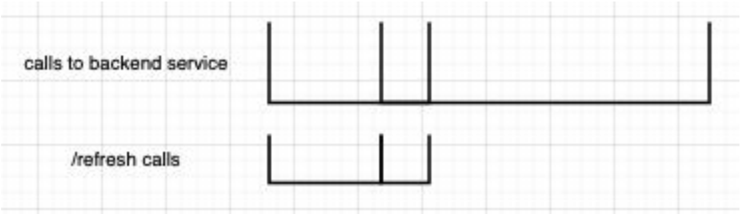
/verify: verifies whether an access token is still valid

Do we always need a refresh, and an access token?

Modes of (Client-Side) Session Elongation

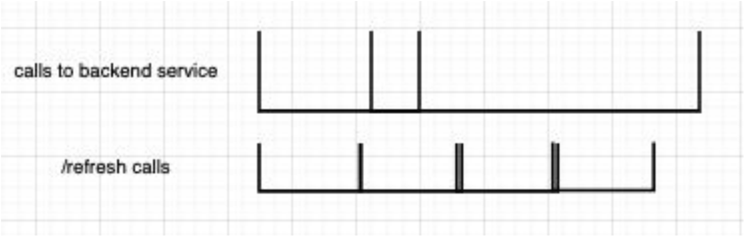
A.

Calling /refresh on every backend call



B.

Frontend will call /refresh periodically



Between the Storages

Type	Local Storage	Session Storage	Cookie	GlobalThis
Space Size	5MB (min)	5MB (min)	4KB (max)	Browser Storage
Properties	Domain access	Domain access	Domain and subdomain access	Domain access
Removal	Clear browsing data	Close tab	Set Expiration	Clear browsing data

Standard Ways to Protect a Cookie

httpOnly flag (prevents client-side access; for server-side cookies)

SameSite=strict (prevents CSRF)

secure=true (only sends cookies on HTTPS protocol)

Backend vs Frontend Calls

User-identifying vs Server-identifying

Authentication vs Authorization

What’s Secure, Anyway?

Encryption vs Masking vs Hashing

User Requirements

- Coming back to the login page to be auto-redirected to a post-login landing page if currently logged in.
- If you already had a login page open - clicking on login button should through-train into the application.
- Should a user be logged in when they open a different tab in the same browser?
    - Will determine where you store your session token - in localStorage, globalThis, Redux, Cookies (more work needed)

Why All The Redirects, Anyway

- Different Authenticating Service (for e.g. SPCP)
- Mysterious, it is

Puzzles

Non Comprendo - “Protocol Fatigue”

- Why do we need so many standards/protocols?
- How are they different?
- What differing functions do they serve?
- Do people earn money when they make a new standard?
- What qualifies as a “new standard”?
- What is the meaning of life?

[Optional] Errors

- Why don’t people recognize you as being authenticated

The End