

**ConFoo** February 27 2025

---

# OAuth, and trustworthy AI agents that don't terminate humans



**Andrew Lavers**  
Principal Software Developer

**Feedback here:**

<https://confoo.ca/en/2025/feedback/C589391CE079D898B92632FEA4D77BB4>



# I work on customer support software at Zendesk in Montreal

The image displays two side-by-side screenshots of customer support software interfaces.

**Left Screenshot:** A web-based help center interface. At the top, there is a search bar containing the placeholder text "##- Please type your reply above this line -##". Below the search bar, the page title is "Help Centre". The navigation menu includes "Get Started", "Move Money", "Investing", "Spend", "File Taxes", "Your Profile", "Log in", and a yellow "Get started" button. The main content area features a heading "How can we help?", a search bar with the placeholder "Search for your question", and a section titled "Find information by topic" with three cards: "Get Started" (with an icon of a gold coin), "Big Winter Bundle Promotion" (with an icon of three coins), and "Move Money" (with an icon of a gold coin).

**Right Screenshot:** A mobile-style help center interface titled "Minecraft Help Center". The header includes a magnifying glass icon and the title "Minecraft Help Center". The timestamp "12:08 PM" is shown. A message from a user named "Minecraft Help" says: "Hi there. Got a question? I'm here to help. Pick an option below or feel free to ask a question." Below the message, a profile picture of a green creeper is visible. A timestamp "Just now" is shown next to the message. A list of support options is displayed in green rounded rectangles: "Minecraft Realms", "Refunds", "Report a Player or Realm", "Technical Support", "Marketplace", and "Account Issues". At the bottom, there is a text input field labeled "Type a message" and a green send button with a downward arrow.

# AI is a big deal at Zendesk

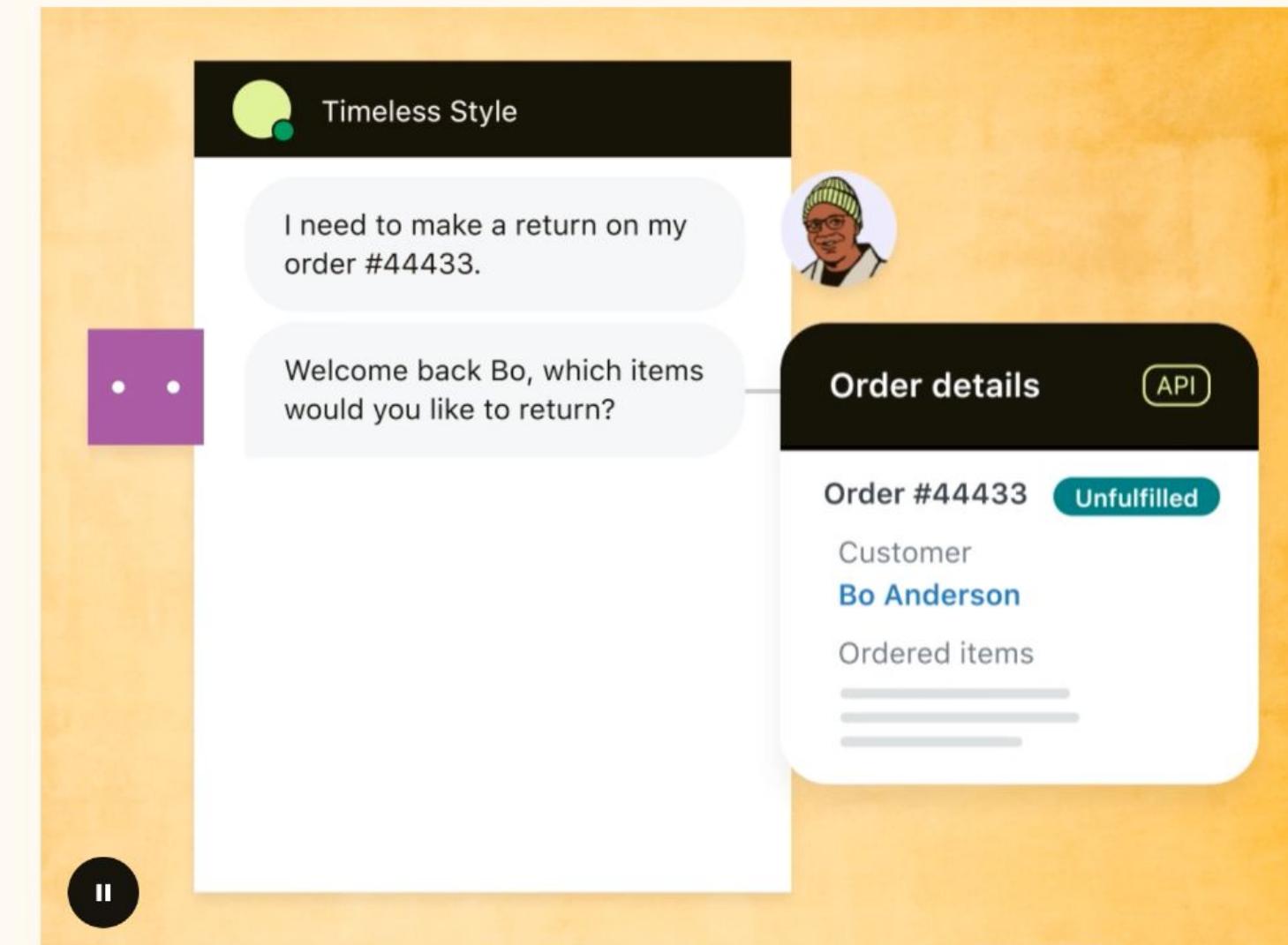
*(this talk isn't a Zendesk ad, I promise)*

AI-POWERED BOTS

## Reach +80% automation across every channel

Zendesk AI agents can understand and resolve the most sophisticated interactions from end to end. Delight your customers with instant, personalized support that's always on—while reducing costs at scale.

[Check out AI agents](#)





The  
customer  
is always  
human



AI is real,  
it's also a bubble

# Nikhil Suresh

<https://ludic.mataroa.blog/blog/i-will-fucking-piledrive-you-if-you-mention-ai-again/>

« Ludicity

## I Will Fucking Piledrive You If You Mention AI Again

Published on June 19, 2024

The recent innovations in the AI space, most notably those such as GPT-4, obviously have far-reaching implications for society, ranging from the utopian eliminating of drudgery, to the dystopian damage to the livelihood of artists in a capitalist society, to existential threats to humanity itself.

I myself have formal training as a data scientist, [going so far as to dominate a competitive machine learning event at one of Australia's top universities](#) and writing a Master's thesis where I wrote all my own libraries from scratch in MATLAB. I'm not God's gift to the field, but I am *clearly* better than most of my competition - that is, practitioners like myself who haven't put in the reps to build their own C libraries in a cave with scraps, but can read textbooks, implement known solutions in high-level languages, and use libraries written by elite institutions.

So it is with great regret that I announce that the next person to talk about rolling out AI is going to receive a complimentary chiropractic adjustment in the style of Dr. Bourne, i.e, I am going to fucking break your neck. I am truly, deeply, sorry.

### I. But We Will Realize Untold Efficiencies With Machine L-

What the *fuck* did I just say?

## Nikhil Suresh

<https://ludic.mataroa.blog/blog/i-will-fucking-piledrive-you-if-you-mention-ai-again/>

A second outcome is that it turns out that the current approach does not scale in the way that we would hope, for myriad reasons. There isn't enough data on the planet, the architecture doesn't work the way we'd expect, the thing just stops getting smarter, context windows are a limiting factor forever, etc.

In this universe, *some* industries will be heavily disrupted, such as customer support.

AI Agents do not **re**place  
human agents,  
it **dis**places them

Ask about CORPORATE SERVICES

May I Suggest:

- MONEY
- TRAVEL
- HEALTH
- COMPUTERS
- ENTERTAINMENT
- FAMILY
- SHOPPING
- ASK JEEVES FOR KIDS!
- JUST CURIOUS, JEEVES

Ask Jeeves Ask.com

Have a Question?  
Just type it in and click Ask!

Most Recent Questions About Jobs:

Where can I find career information and advice about becoming a television

What are people asking RIGHT NOW? →

Ask!

Make Jeeves Your Homepage • Play a Game • Advertise On Jeeves • Become an Affiliate • Investor Relations

© 1996-1999 Ask Jeeves, Inc.  
ASK JEEVES, ASK.COM and the JEEVES DESIGN are service marks of Ask Jeeves, Inc.  
All other brands are property of their respective owners. Patent pending.

## NATIONAL PORTRAIT GALLERY

Shop Donate Search

Visit What's on Explore our Collection Learn Membership

Home / About us / FAQ

# FAQ

---

## General information

Frequently asked questions mainly relating to opening hours and location information.

**Where is the National Portrait Gallery?**

**How do I get to the National Portrait Gallery?**

**What are the Gallery's opening hours?**

**Is photography allowed in the Gallery?**

**Who can I contact about lost property?**

**Can I sketch in the Gallery?**

**How can I be put on your mailing list?**

**Can I link to your website?**

---

## Facilities

Frequently asked questions mainly relating to the Gallery's building and facilities.

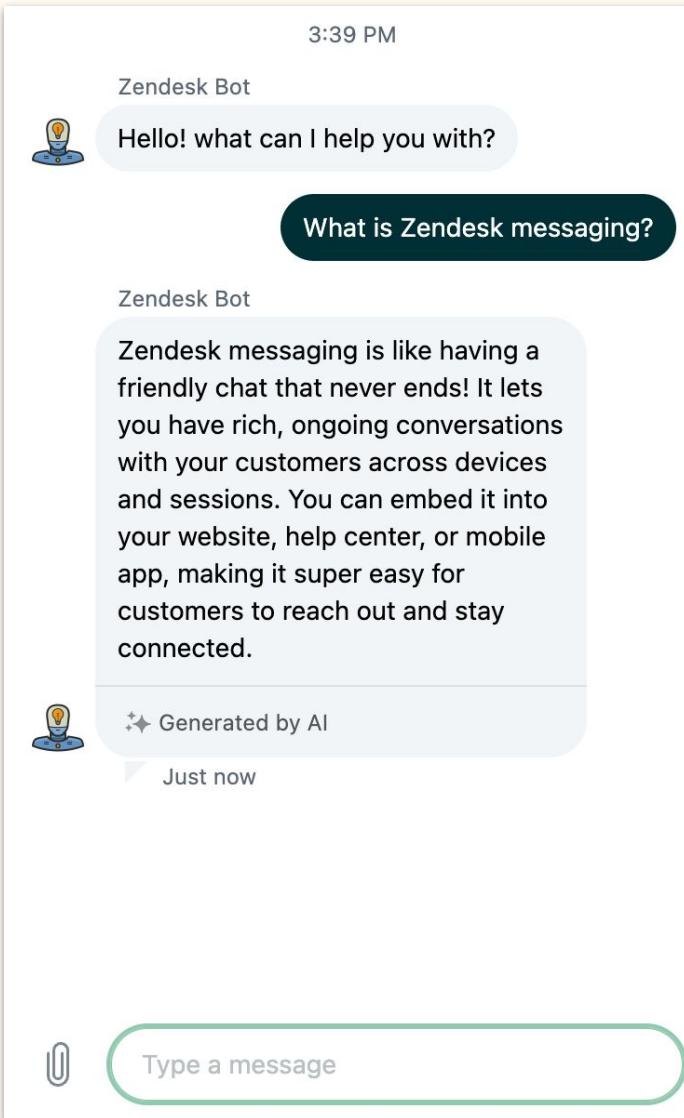
**Do you have a map of the Gallery?**

AI Agents =  
self-serve support

# Generative AI in customer support

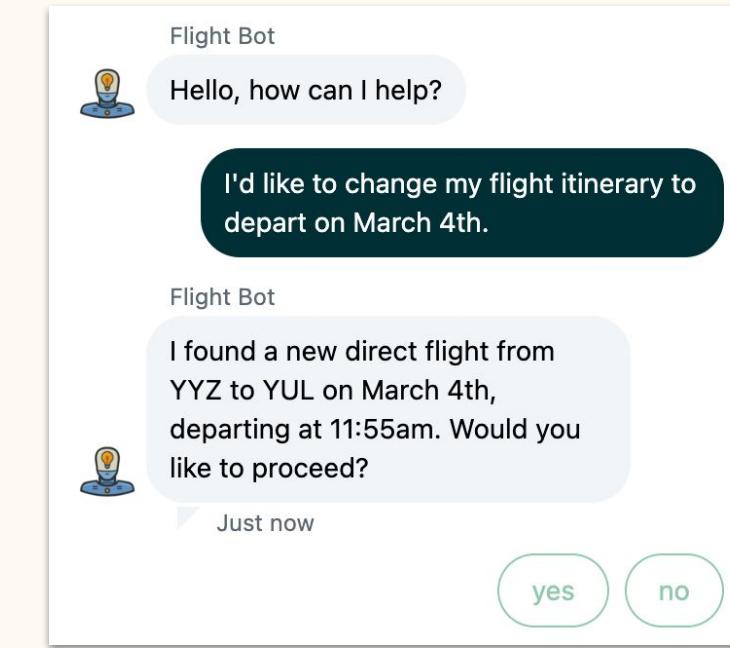
## 1. Answering questions

(RAG, Retrieval Augmented Generation)



## 2. Solving problems

(Reasoning engines connected to APIs)

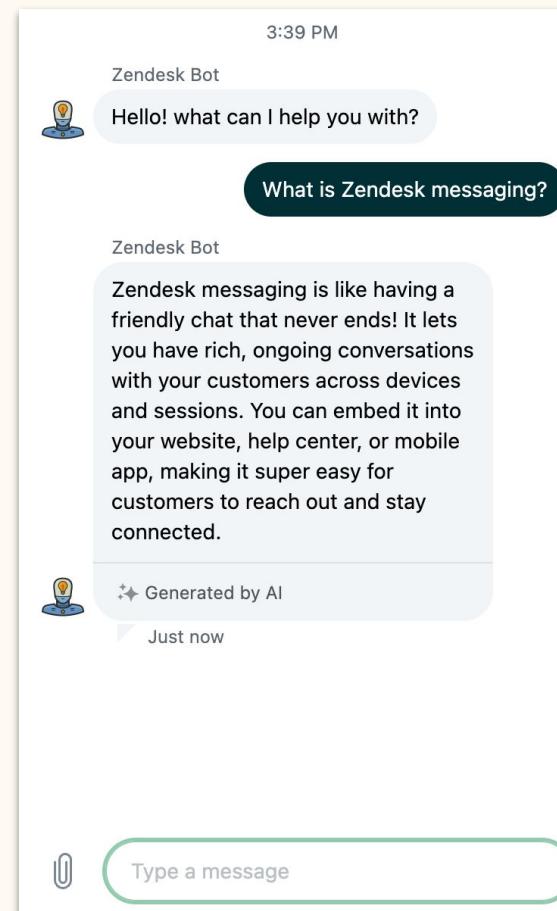


# Generative AI in customer support

## 1. Answering questions

(RAG, Retrieval Augmented Generation)

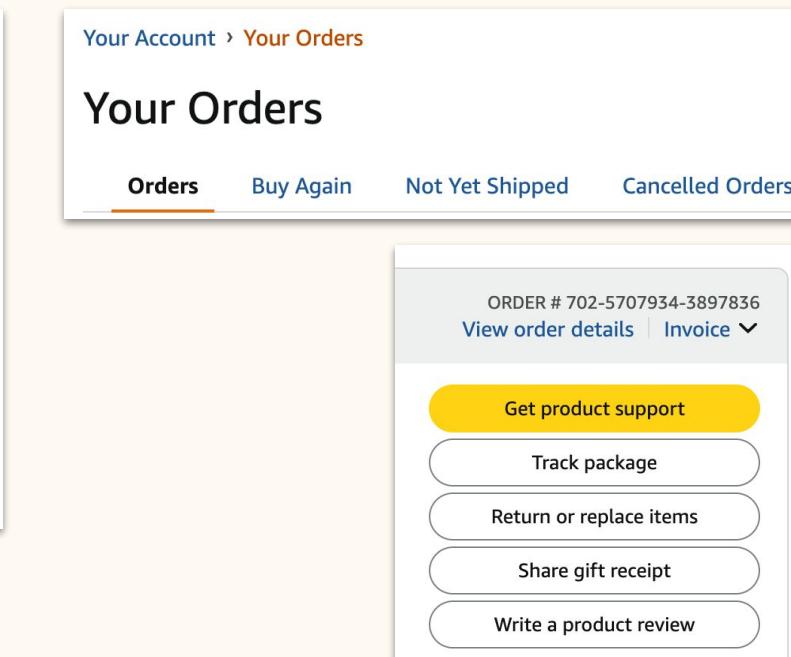
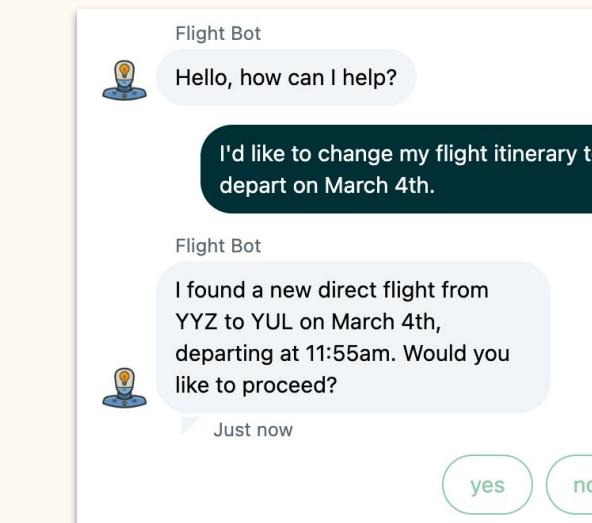
- Conversational knowledge base
- Open to everyone



## 2. Solving problems

(Reasoning engines connected to APIs)

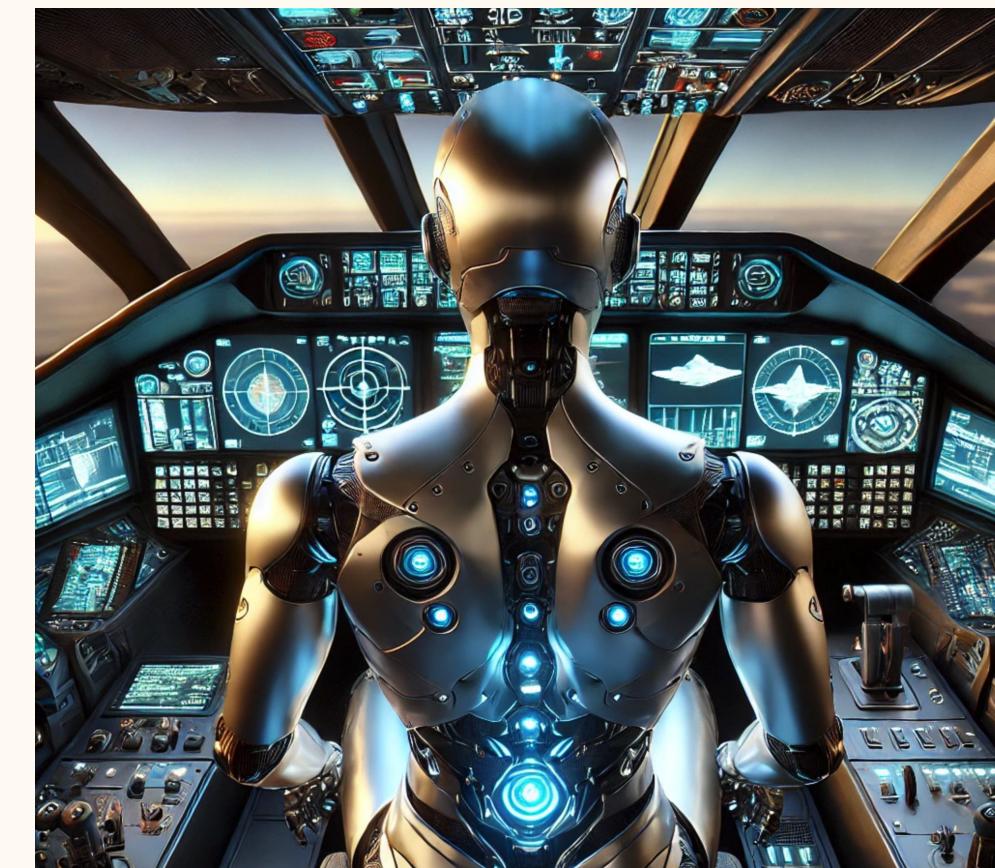
- Conversational **self-serve UI**
- **Requires user authentication**



**Bots are not human shaped**

# Car insurance without a human driver







# Viewing a bot-controlled support ticket

What goes into the assignee field?

The screenshot shows a Zendesk support ticket interface for "Ticket #39". The top navigation bar includes "Organization (create)", "Andrew Lavers", and "Open Ticket #39".

**Requester:** Andrew Lavers

**Assignee\***: Zendesk Bot (highlighted with an orange border)

**Followers:** (empty)

**Tags:** (empty)

**Type:** -

**Priority:** -

**Conversation with Andrew Lavers (Via messaging):**

- Zendesk Bot** (40 minutes ago): Hello! what can I help you with?
- Andrew Lavers** (39 minutes ago): What is Zendesk messaging?
- Zendesk Bot** (39 minutes ago): Zendesk messaging is like having a friendly chat that never ends! It lets you have rich, ongoing conversations with your customers across devices and sessions. You can embed it into your website, help center, or mobile app, making it super easy for customers to reach out and stay connected.

**Profile of Andrew Lavers:**

- Local time: Fri, 16:19 EST
- Language: English (United States)
- Notes: Add user notes

**Device information:** (collapsible)

**Interaction history:**

- Conversation with Andrew Lavers (38 minutes ago, Status Open)

# *Bots are not human shaped*



One does not simply route an incoming support request to a human. Human agents:

- Are organized into pools by skill, channel, and region
- Have availability and capacity
- Are a **finite resource**
- Have their performance measured by things like:
  - FRT = First Response Time

This **human-shaped work** is governed by the Assignee field ➡

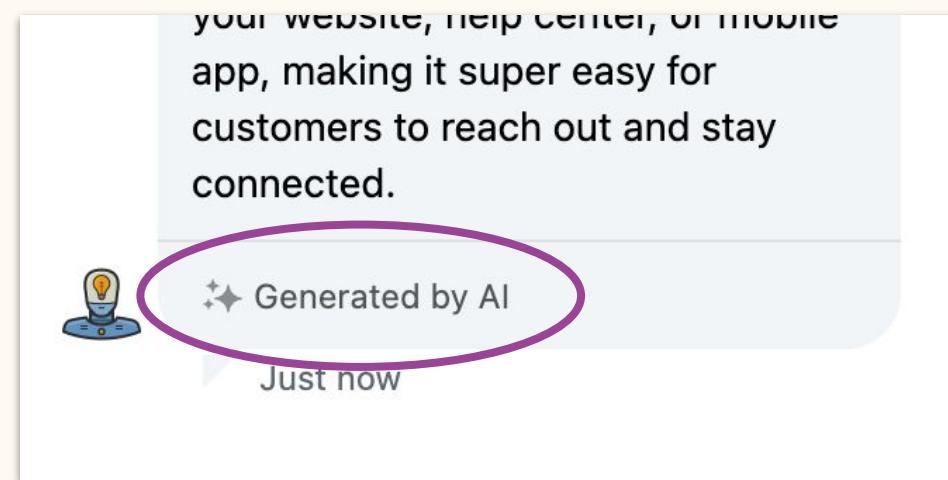
Organization (create)	Andrew L
Requester	
Andrew Lavers	
Assignee*	<a href="#">take it</a>
<input type="button" value="▼"/>	



Bots are not human shaped  
Do not put bots into human-shaped interfaces

-  ~~Androids in cockpits~~
-  Build drones

# Accept bots for what they are



Do not try to fool the end user  
into thinking your bot is a human

*The end user will figure it out*

**Generative AI is not a silver bullet  
Use the right tool for the job**



# Generative AI is not a silver bullet

## Use the right tool for the job



### Generative AI

- Powerful dynamic reasoning capabilities
- Unpredictable
- Planning a new flight itinerary

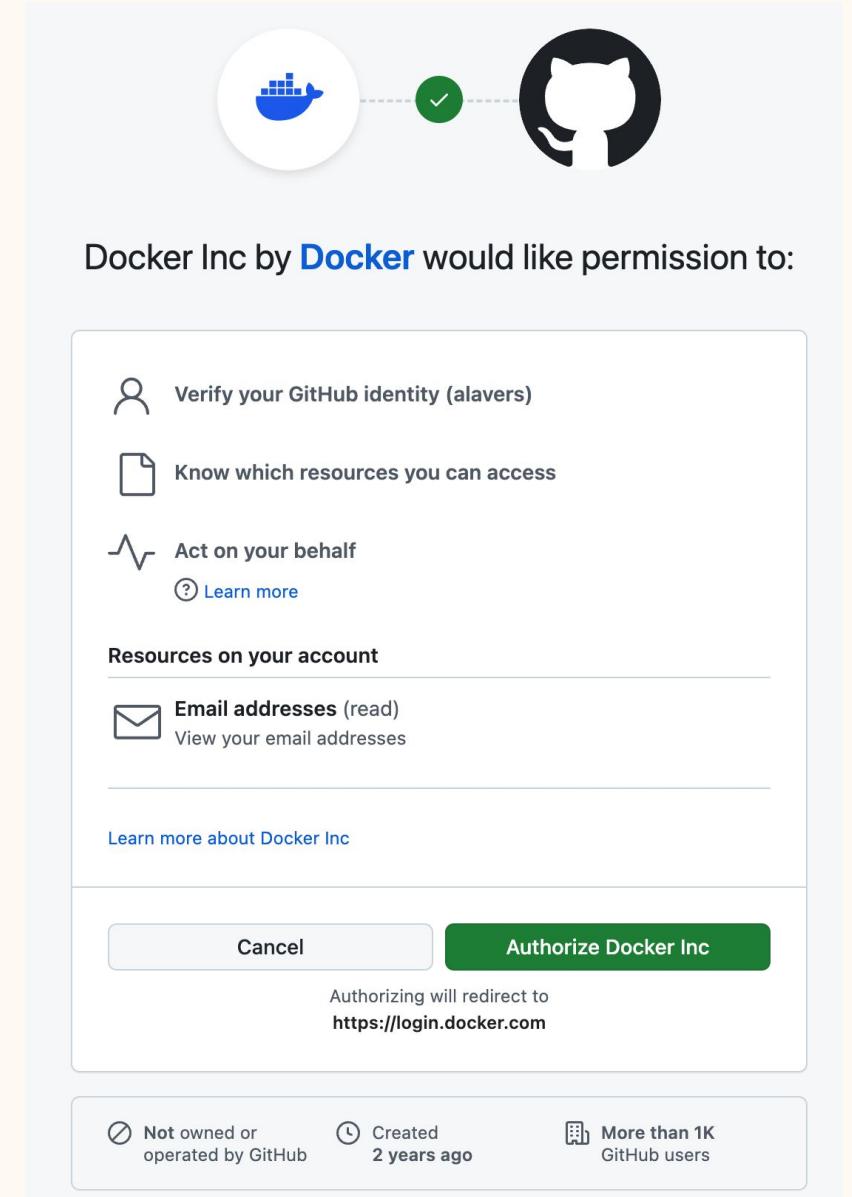
### Deterministic code

- Rigid logic that must be fully specified in advance
- Predictable
- Authorizing access to view or change flight itinerary

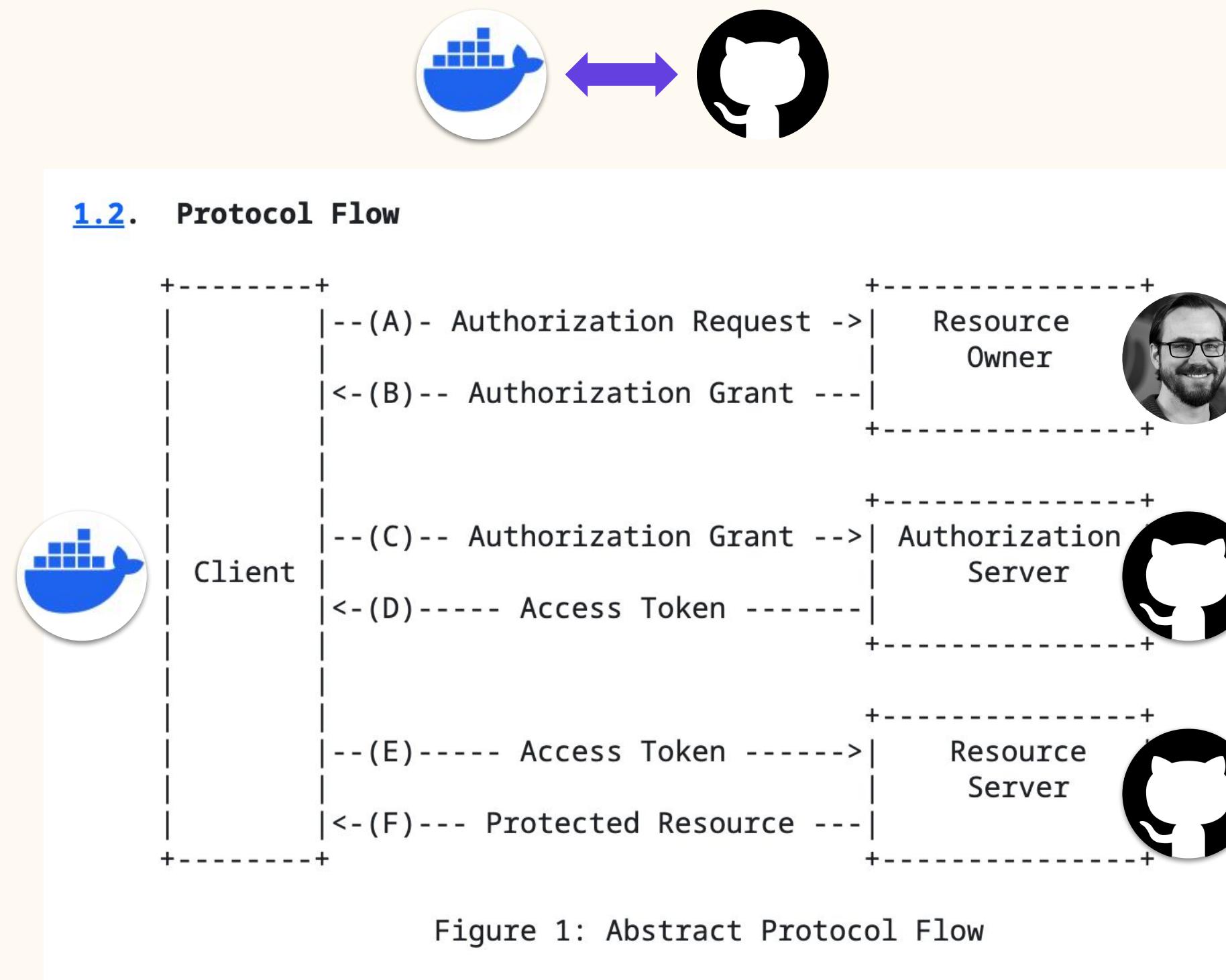


Speaking of deterministic approaches...



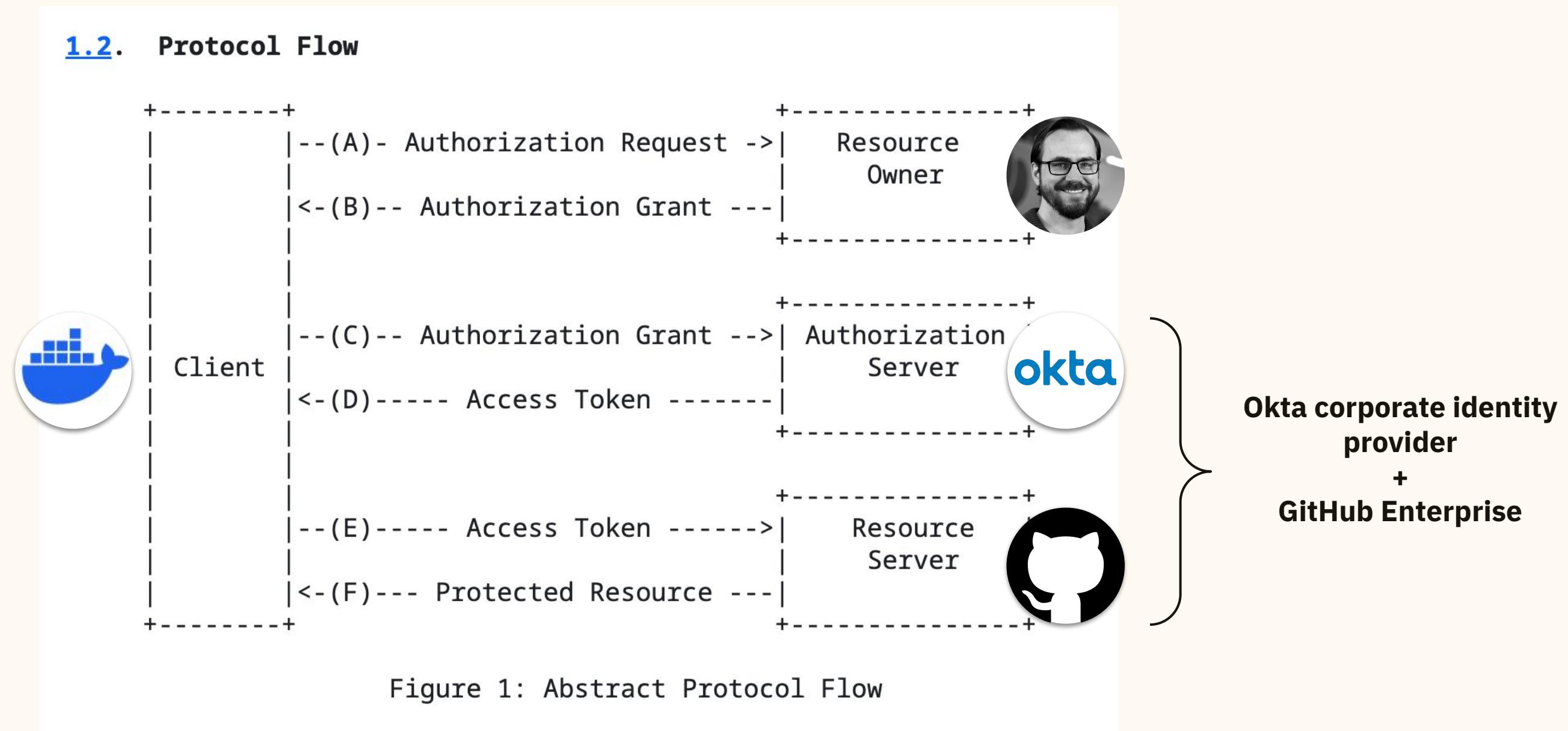


# A brief overview of OAuth



Taken straight from the RFC: <https://datatracker.ietf.org/doc/html/rfc6749>

# A brief overview of OAuth



Taken straight from the RFC: <https://datatracker.ietf.org/doc/html/rfc6749>

15% OFF FIRST ORDER - SIGN UP TODAY

(877) 404 6763

HORNE

TRADE JOURNAL    

NEW FURNITURE LIGHTING OUTDOOR KITCHEN + DINING BED + BATH ACCESSORIES KIDS BRANDS SALE **IN STOCK**

SEARCH 

HORNE Customer Support



HORNE Customer Support Bot

Leave a message and we will email you once we are online.

What can we help you with?

Automated

Track Order

Report Issue

Cancel Order

Product Question

Other



# A brief overview of OAuth

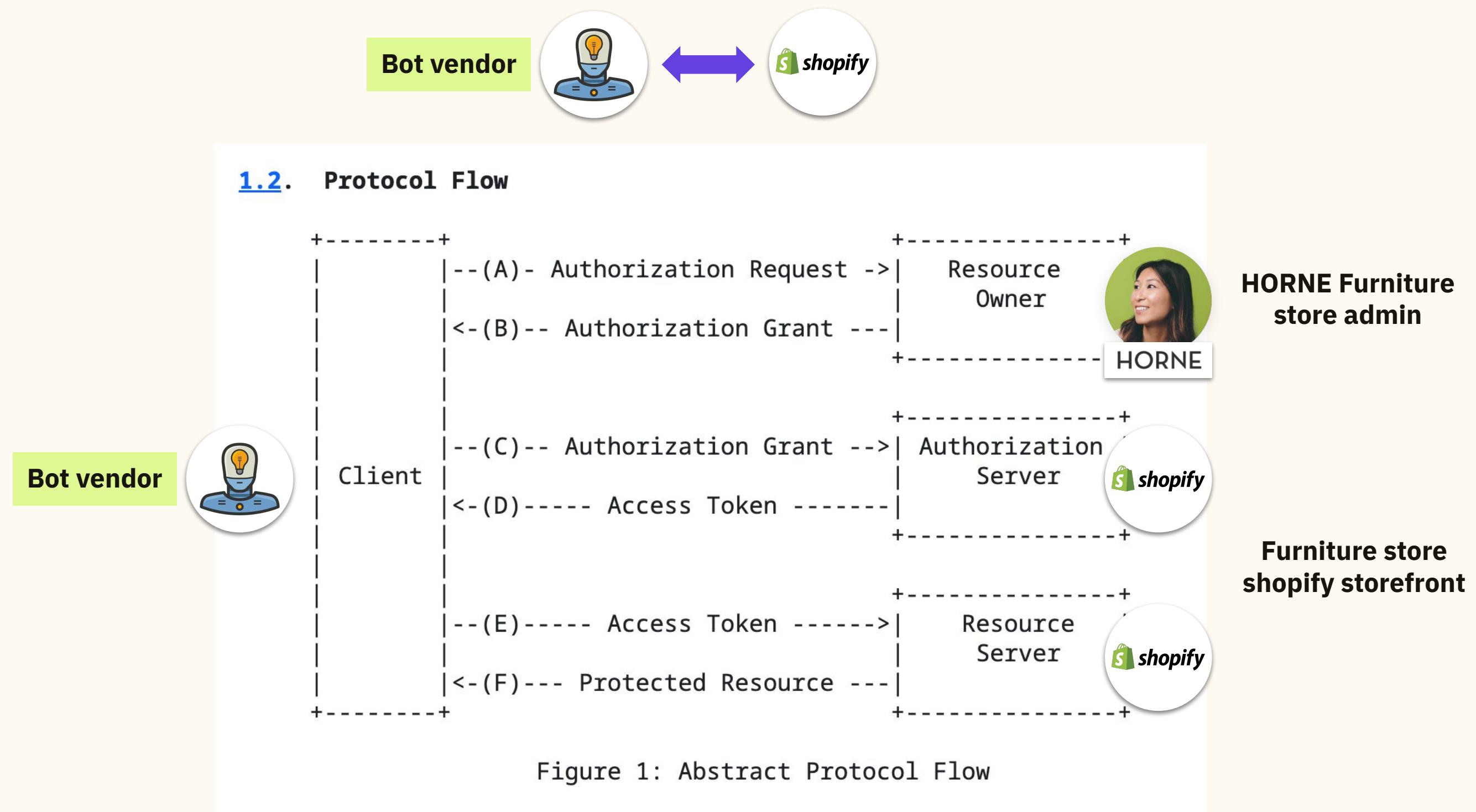
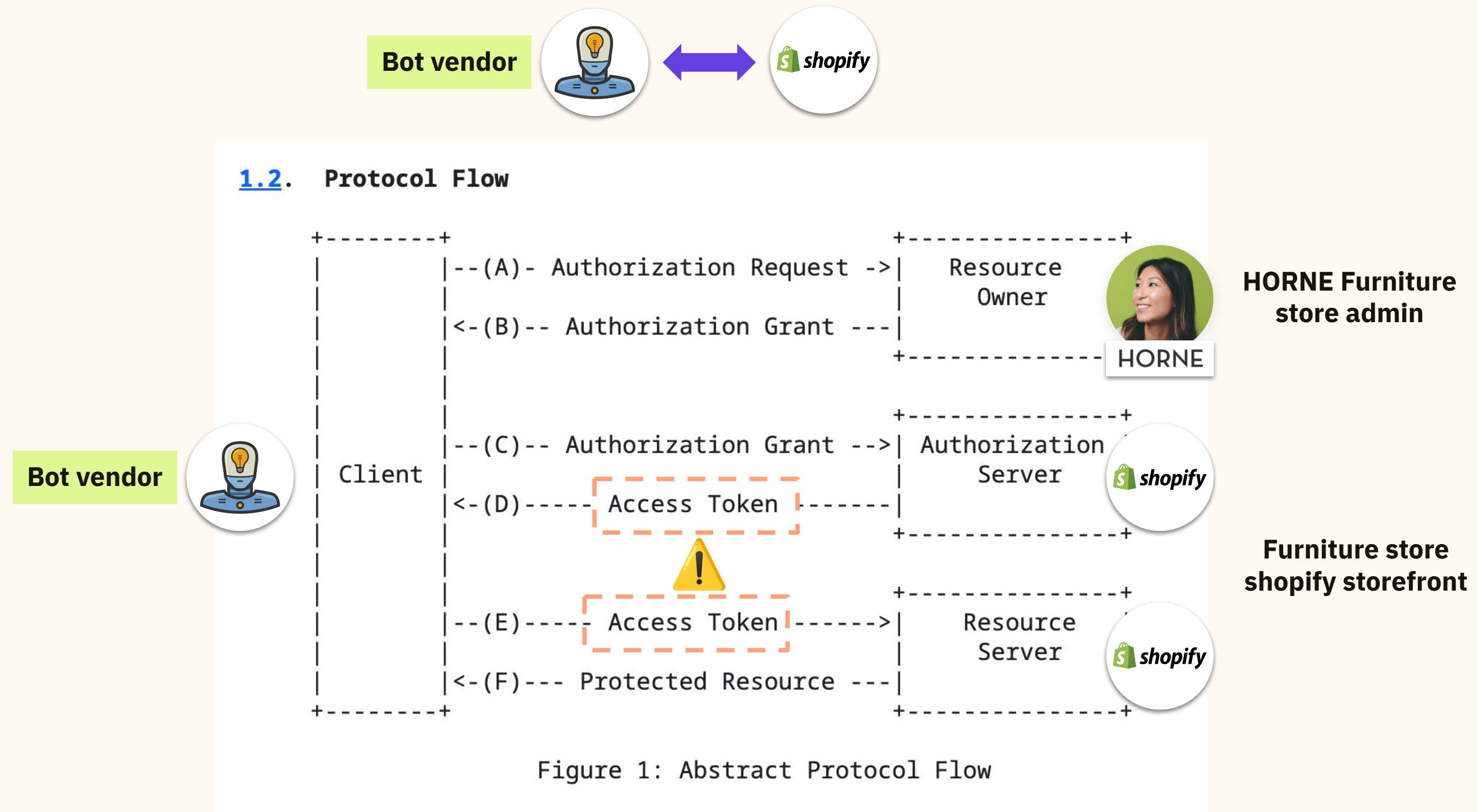


Figure 1: Abstract Protocol Flow

Taken straight from the RFC: <https://datatracker.ietf.org/doc/html/rfc6749>

# A brief overview of OAuth



Taken straight from the RFC: <https://datatracker.ietf.org/doc/html/rfc6749>

an exchange for my order?

Of course! Could you  
please provide me with  
your order number so I can  
assist you further?

I don't know my order  
number but my email is  
[sarah.mitchell@gmail.com](mailto:sarah.mitchell@gmail.com)

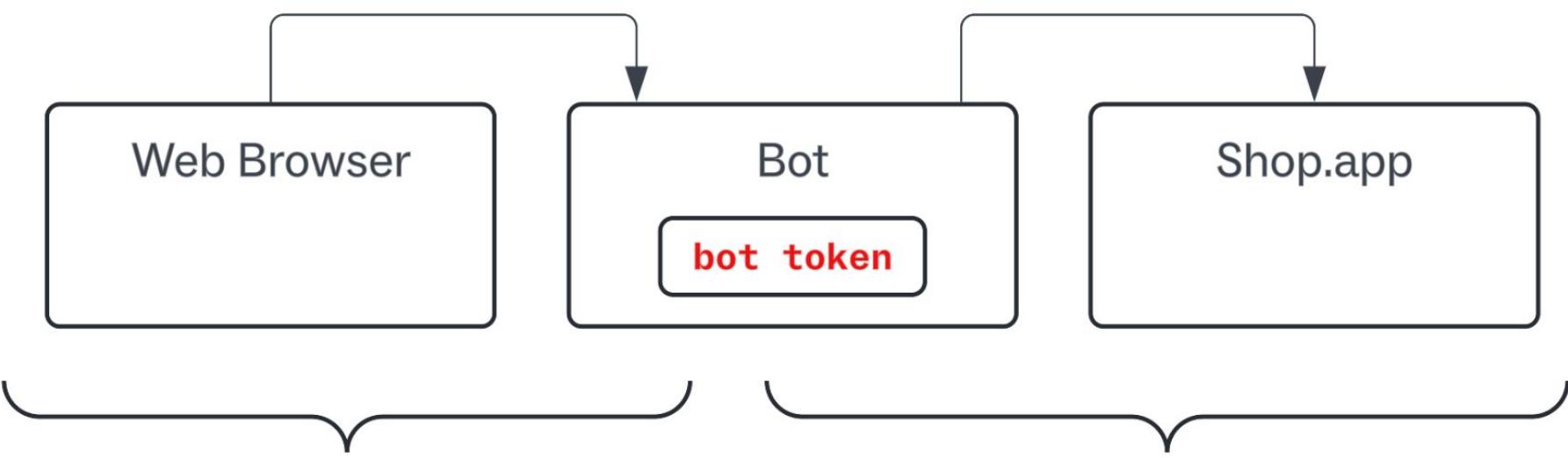
I found your order. Before  
we proceed with the  
exchange, can you confirm  
that your shipping address  
is 6870 Grand Haven Rd,  
Spring Lake, MI, 49456?

Message...

Powered by  Bot vendor

*"My email is sarah.mitchell@gmail.com,  
Please modify my order"*

**GET /orders?email=sarah.mitchell@gmail.com**  
**Authorization: bot token**



Human termination problem

Indemnification problem

an exchange for my order?

Of course! Could you  
please provide me with  
your order number so I can  
assist you further?

I don't know my order  
number but my email is  
[sarah.mitchell@gmail.com](mailto:sarah.mitchell@gmail.com)

I found your order. Before  
we proceed with the  
exchange, can you confirm  
that your shipping address  
is 6870 Grand Haven Rd,  
Spring Lake, MI, 49456?

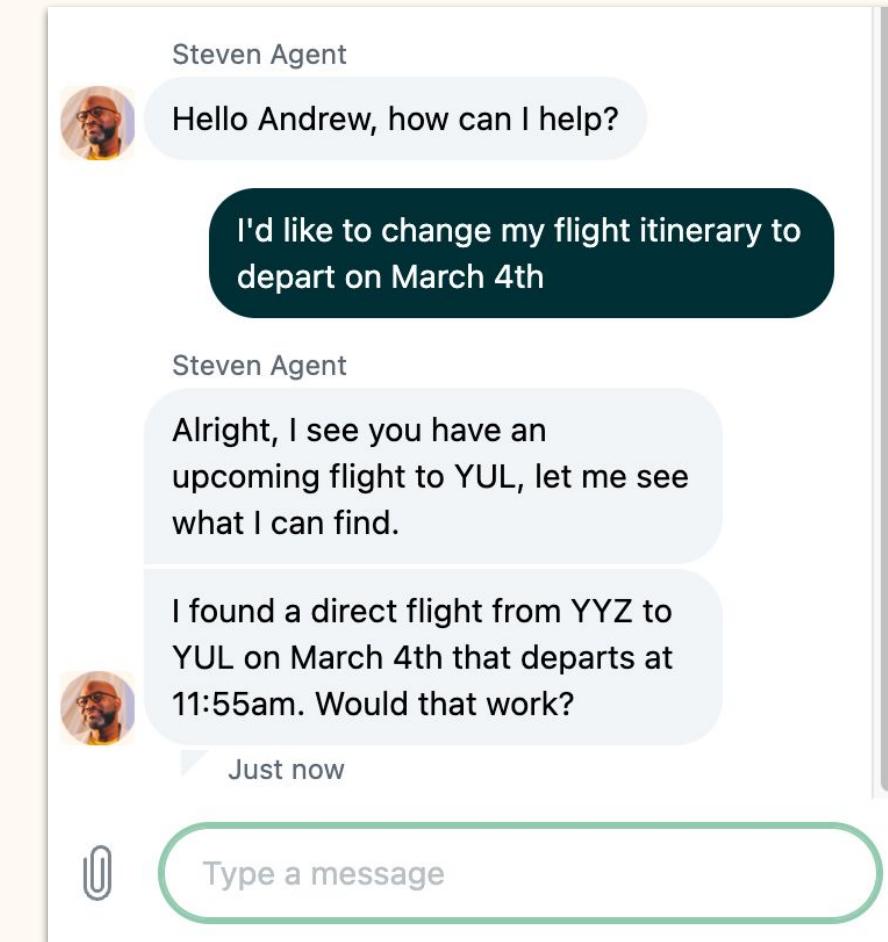
Message...

Powered by Bot vendor

# The question of identities



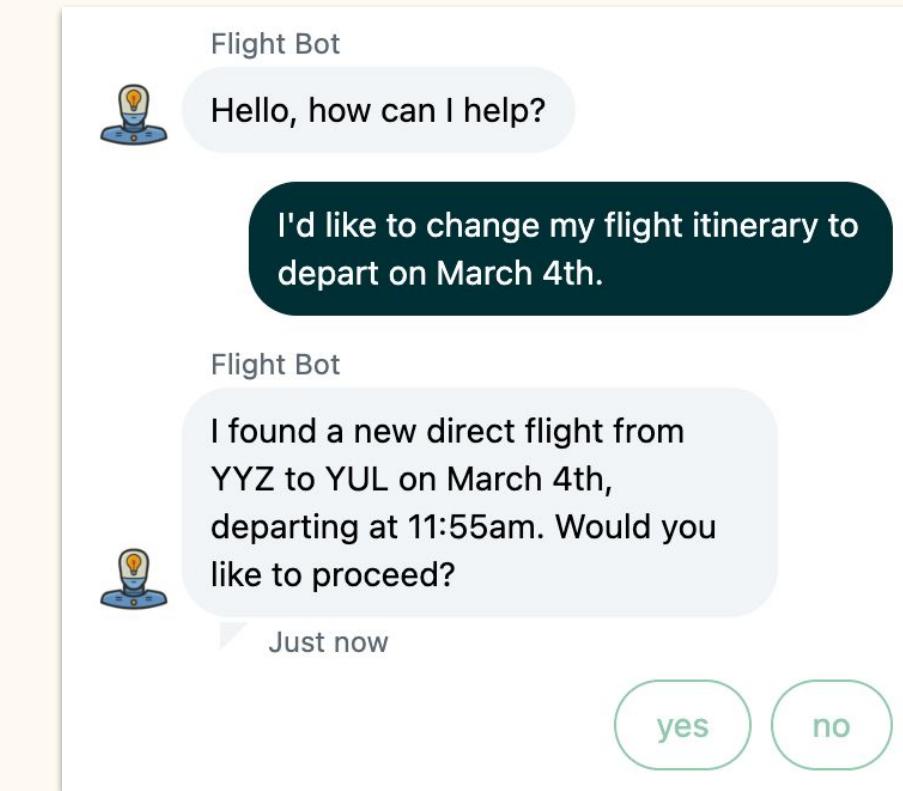
How many **identities** do you see here?



# The question of identities



How many **identities** do you see here?

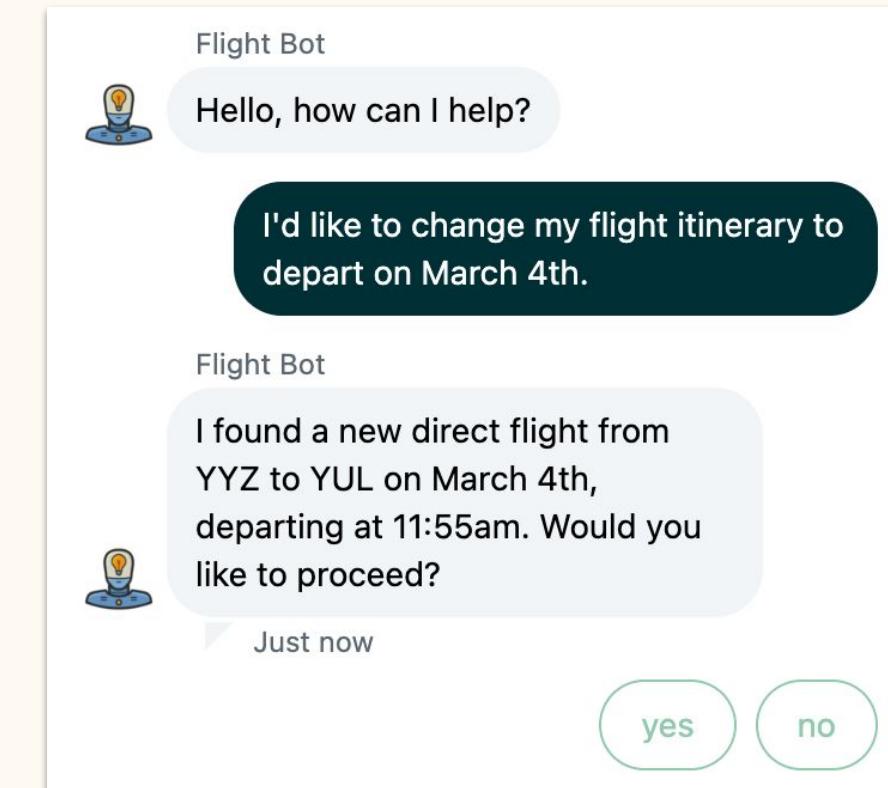


# The question of identities



How many **identities** do you see here?

**Only one**

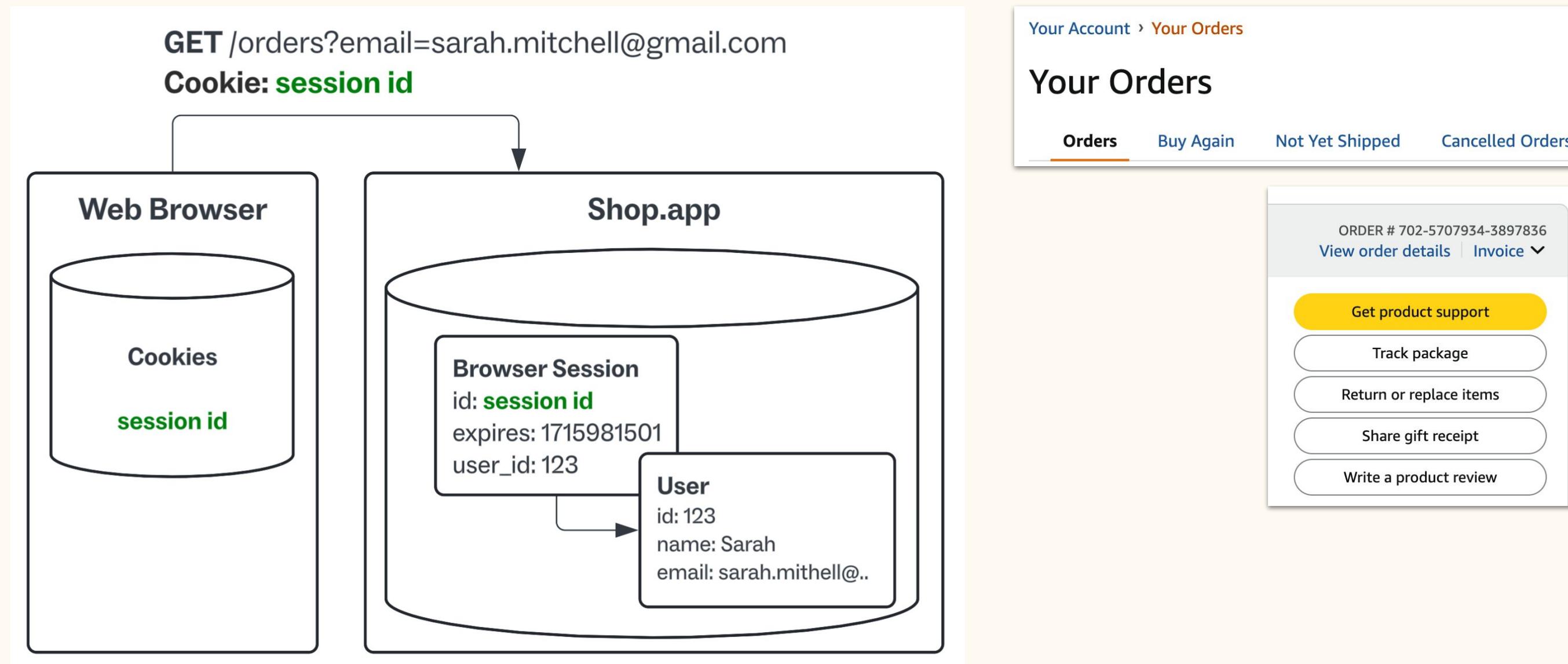


# How do we solve these problems?

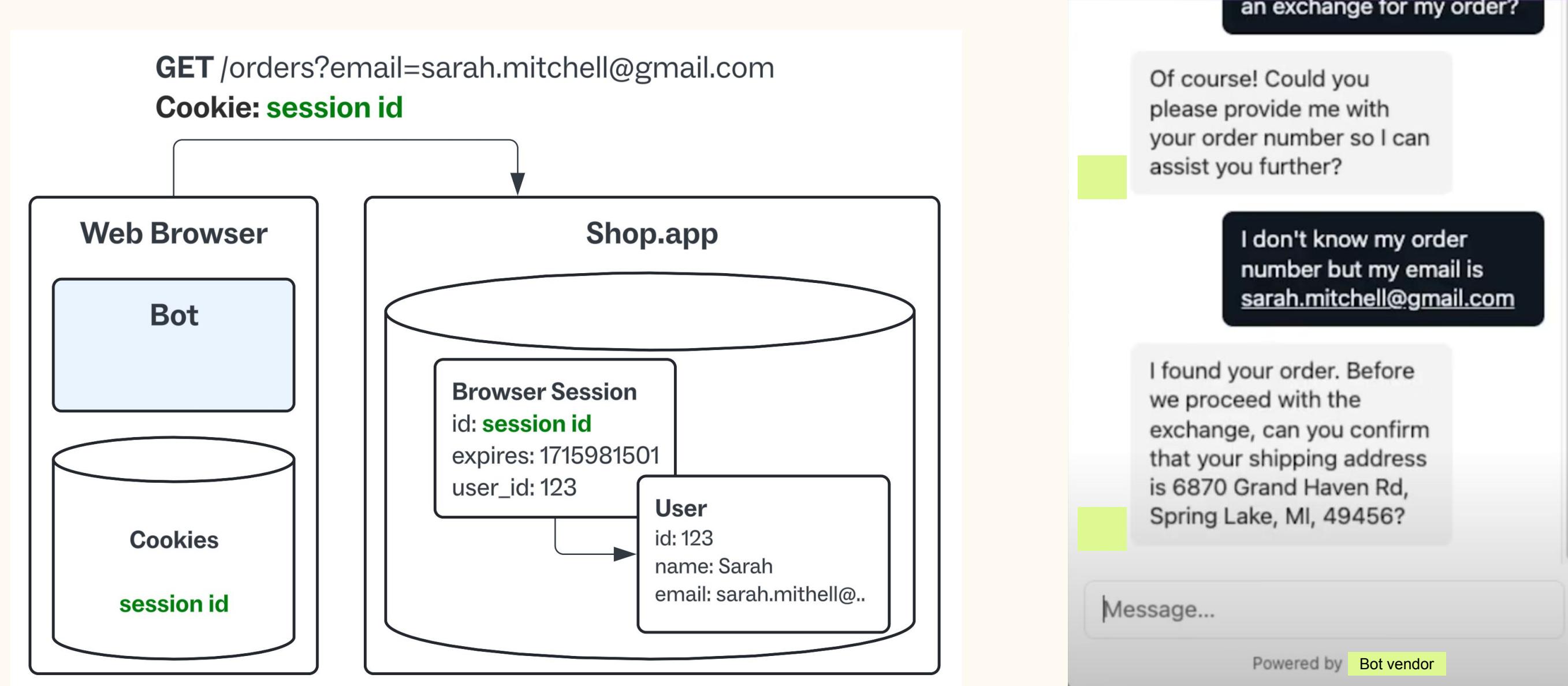
# Let's rewind a bit..



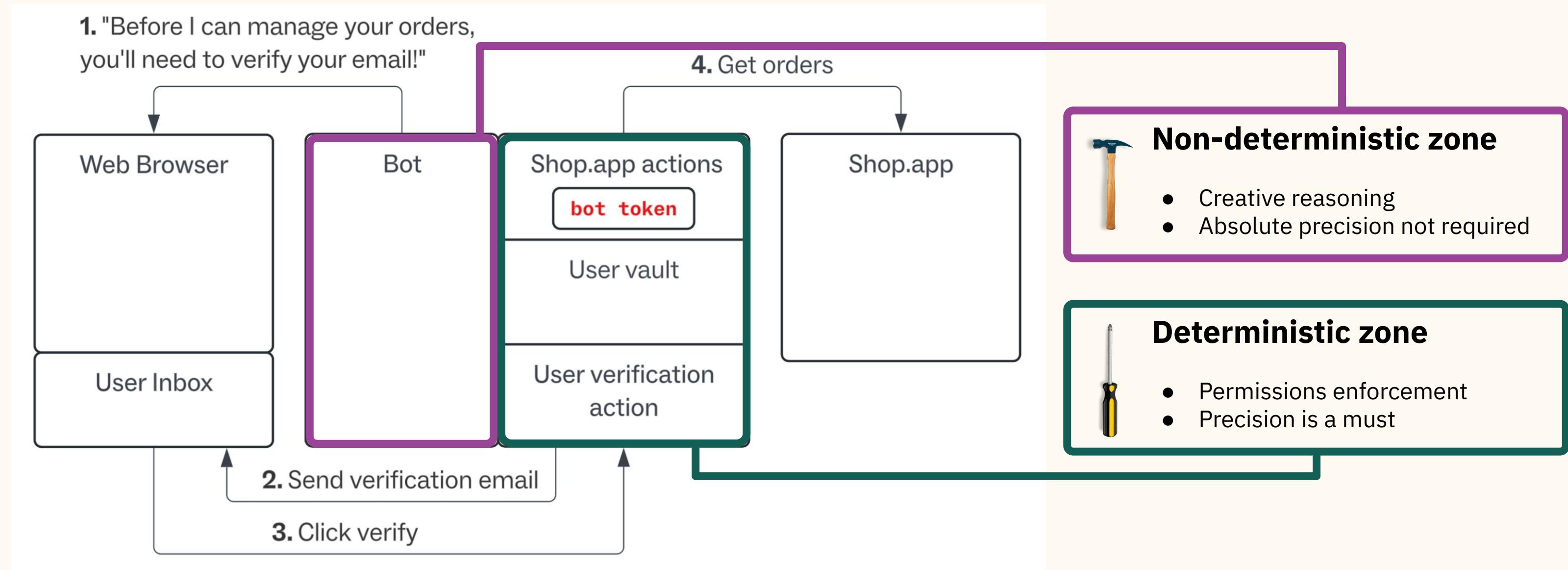
# Browser sessions work quite well



# What if the bot was running in your browser?



# Solution #1: Ad-hoc identity verification



# Can OAuth help?



# Solution #2: OAuth Token Exchange (RFC 8693)

<https://datatracker.ietf.org/doc/html/rfc8693>

Internet Engineering Task Force (IETF)  
Request for Comments: [8693](#)  
Category: Standards Track  
Published: January 2020  
ISSN: 2070-1721

M. Jones  
Microsoft  
A. Nadalin  
Microsoft  
B. Campbell, Ed.  
Ping Identity  
J. Bradley  
Yubico  
C. Mortimore  
Visa

## OAuth 2.0 Token Exchange

### Abstract

This specification defines a protocol for an HTTP- and JSON-based Security Token Service (STS) by defining how to request and obtain security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation.

### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc8693>.

### Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

### 1.1. Delegation vs. Impersonation Semantics

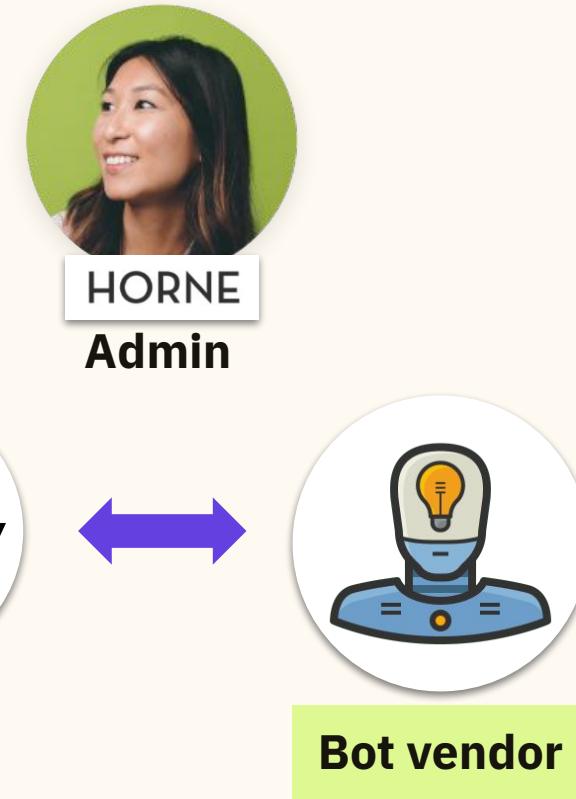
One common use case for an STS (as alluded to in the previous section) is to allow a bot vendor to make calls to shopify orders on behalf of sarah mitchell. Depending on the local site policy and authorization infrastructure, it may be desirable for A to use its own credentials to access C along with an annotation of some form that A is acting on behalf of B ("delegation") or for A to be granted a limited access credential to C but that continues to identify B as the authorized entity ("impersonation"). Delegation and impersonation can be useful concepts in other scenarios involving multiple participants as well.

# Step 1: Setup

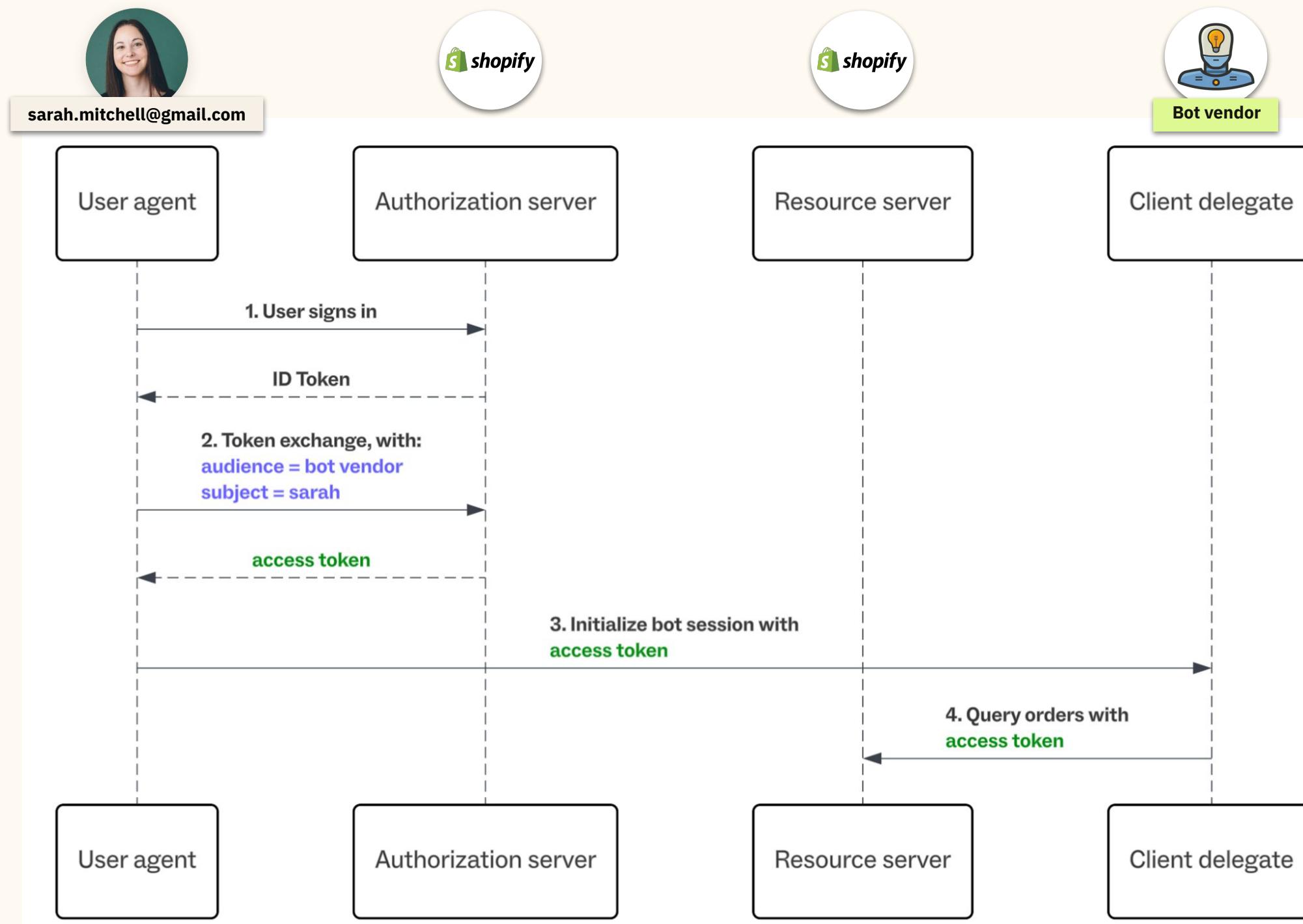
The Shopify storefront admin installs the **bot vendor** as a trusted system.

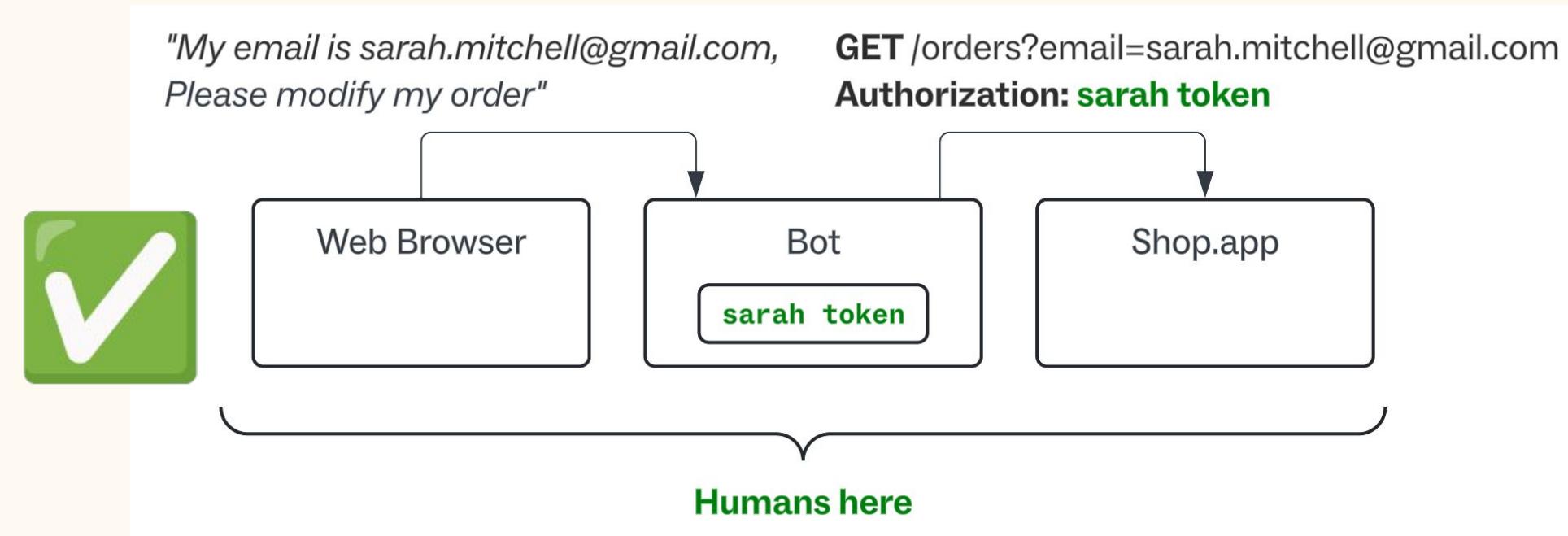
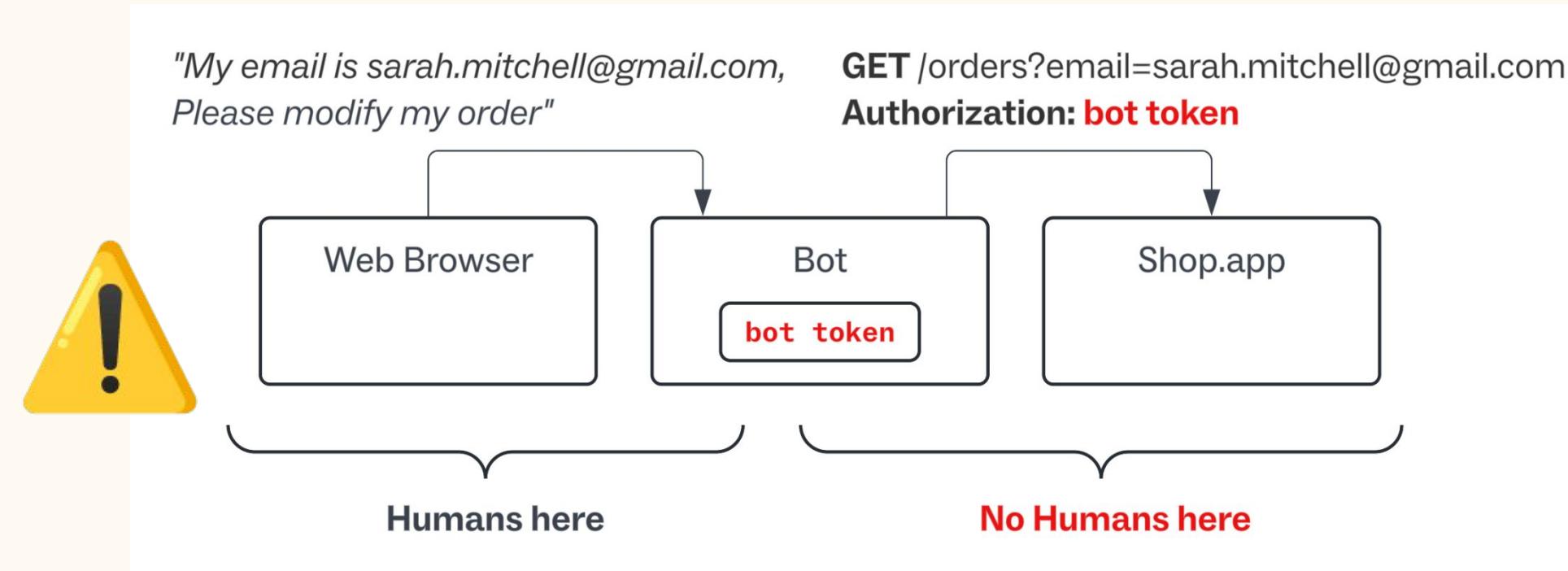
This registers the bot vendor as an **audience** for token exchange.

The bot vendor does not yet have an access token.

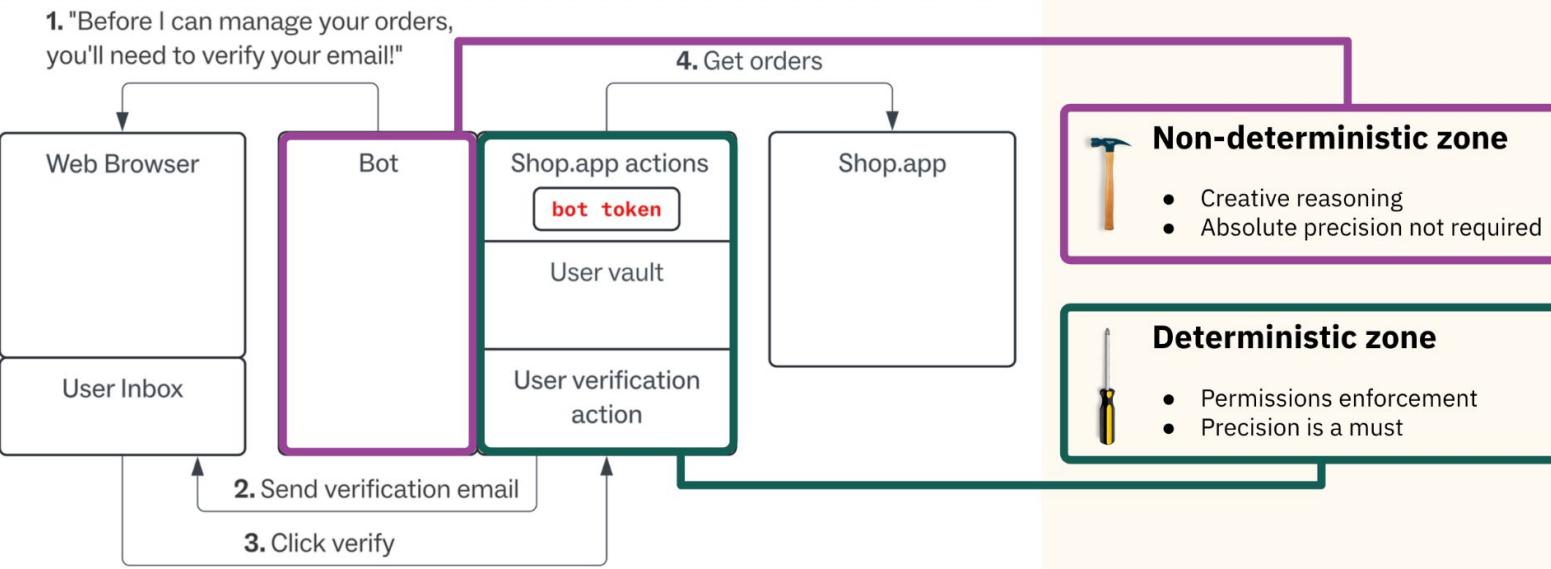


## Step 2: Token exchange





## Solution #1: Ad-hoc identity verification



## Solution #2: OAuth Token Exchange (RFC 8693)

<https://datatracker.ietf.org/doc/html/rfc8693>

Internet Engineering Task Force (IETF)  
Request for Comments: 8693  
Category: Standards Track  
Published: January 2020  
ISSN: 2070-1721

M. Jones Microsoft  
A. Nadalin Microsoft  
B. Campbell, Ed. Ping Identity  
J. Bradley Yubico  
C. Mortimore Visa

**OAuth 2.0 Token Exchange**

**Abstract**

This specification defines a protocol for an HTTP- and JSON-based Security Token Service (STS) by defining how to request and obtain security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation.

**Status of This Memo**

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc8693>.

**1.1. Delegation vs. Impersonation Semantics**

One common use case for an STS (as alluded to in the previous section) is to allow a **bot vendor** to make calls to **shopify orders** on behalf of **sarah mitchell**. Depending on the local site policy and authorization infrastructure, it may be desirable for A to use its own credentials to access C along with an annotation of some form that A is acting on behalf of B ("delegation") or for A to be granted a limited access credential to C but that continues to identify B as the authorized entity ("impersonation"). Delegation and impersonation can be useful concepts in other scenarios involving multiple participants as well.

- Ad-hoc email or phone number verification is an understood pattern
- Can be unilaterally implemented by one party, requires no changes across multiple parties
- Disruptive experience, user has to verify their identity even if they have signed in to the storefront
- Low security posture

- Requires coordination between all parties involved (bot vendor, storefront vendor, identity provider)
- Standards take a long time to adopt, though most identity providers have implemented the token exchange RFC
- Seamless user experience
- High security posture

**ConFoo** February 27 2025

---

# OAuth, and trustworthy AI agents that don't terminate humans



**Andrew Lavers**  
Principal Software Developer

**Feedback here:**

<https://confoo.ca/en/2025/feedback/C589391CE079D898B92632FEA4D77BB4>



**zendesk**