20TH ANNIVERSARY EDITION

WSO2CON ASIA

PLATFORMLESS MODERNIZATION

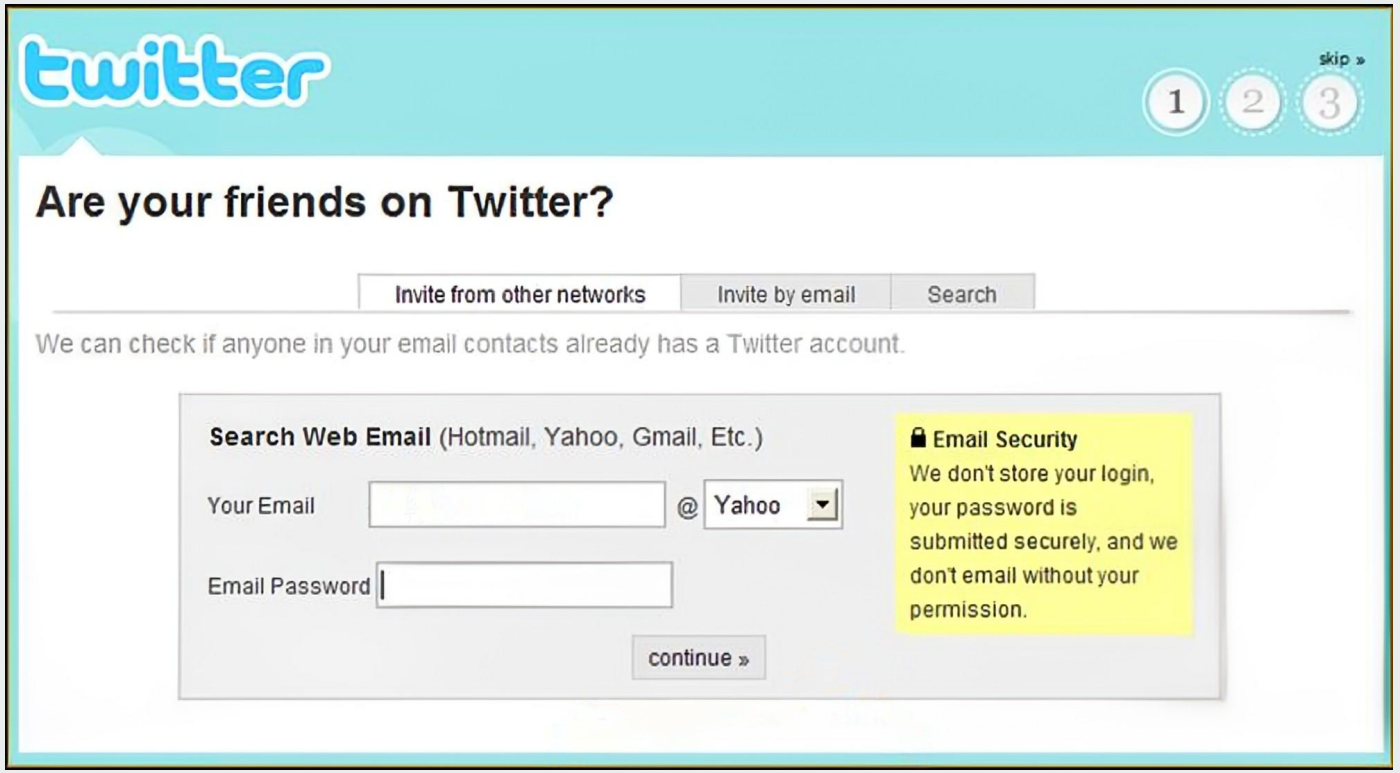
The State of OAuth:

A Guide to New and Upcoming Standards

Janak Amarasena

Technical Lead

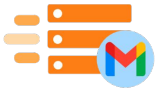
WSO2


twitter
skip »
1
2
3
Are your friends on Twitter?
Invite from other networks
Invite by email
Search
We can check if anyone in your email contacts already has a Twitter account.
Search Web Email (Hotmail, Yahoo, Gmail, Etc.)
Your Email
@
Yahoo
Email Password
continue »
Email Security
We don't store your login, your password is submitted securely, and we don't email without your permission.

How can systems talk to each other without sharing passwords?

How OAuth Solved Credential Sharing: Access Delegation

Twitter

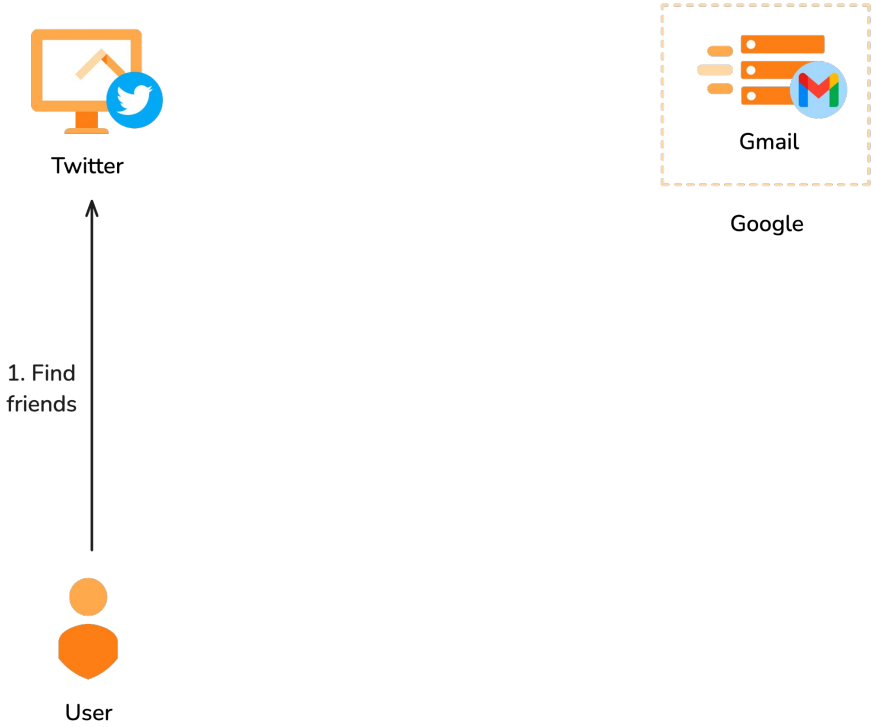


Gmail

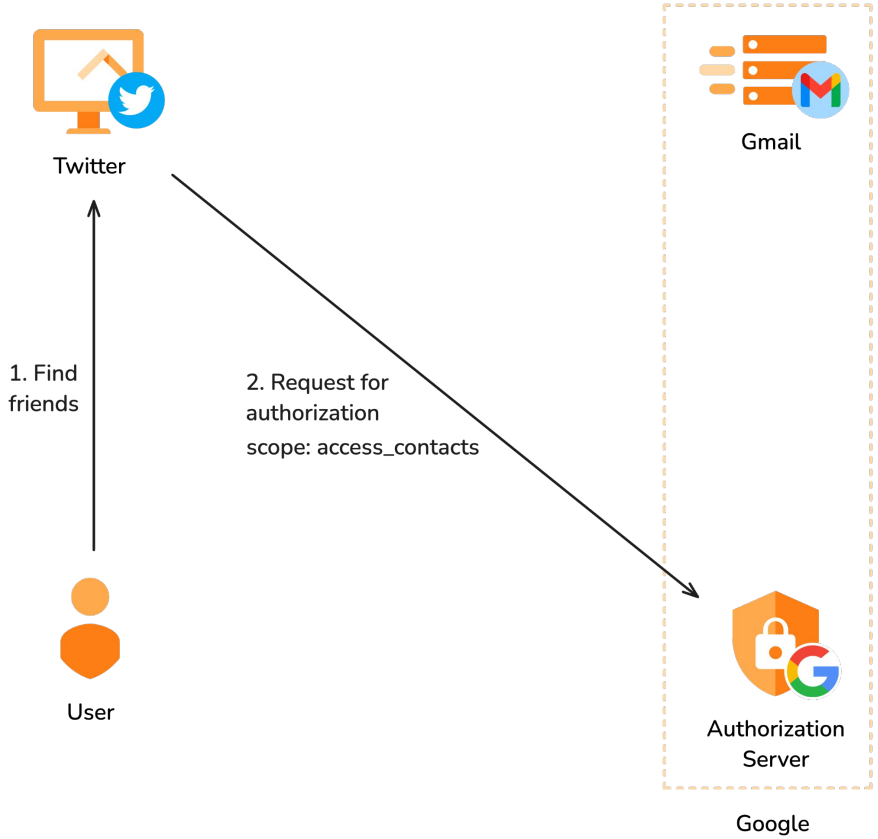
Google

User

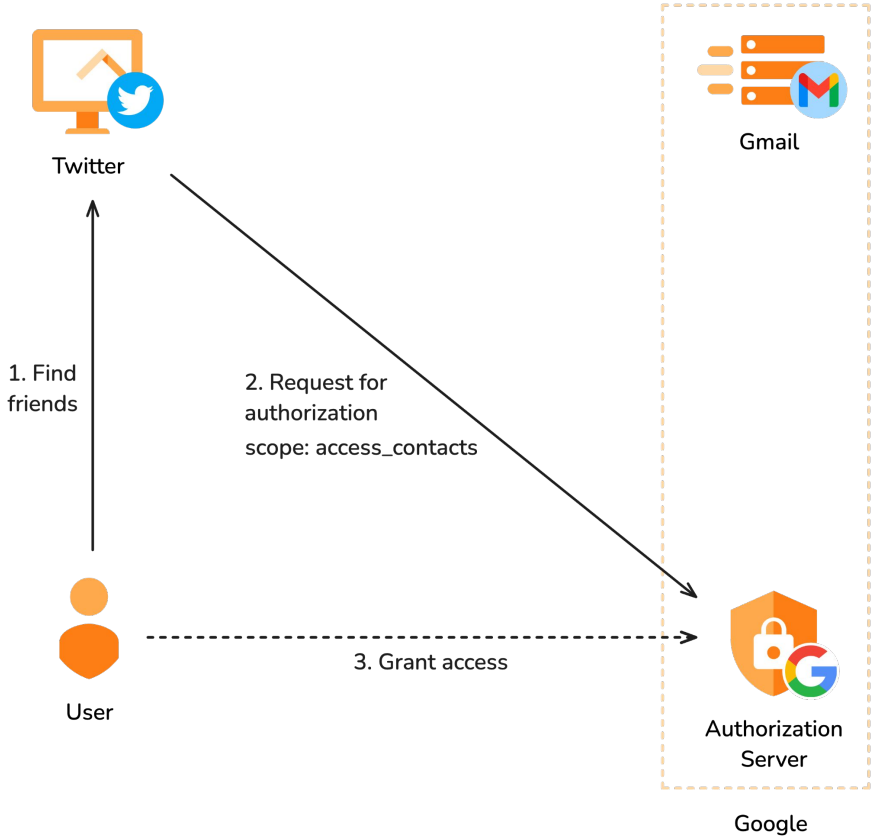
How OAuth Solved Credential Sharing: Access Delegation



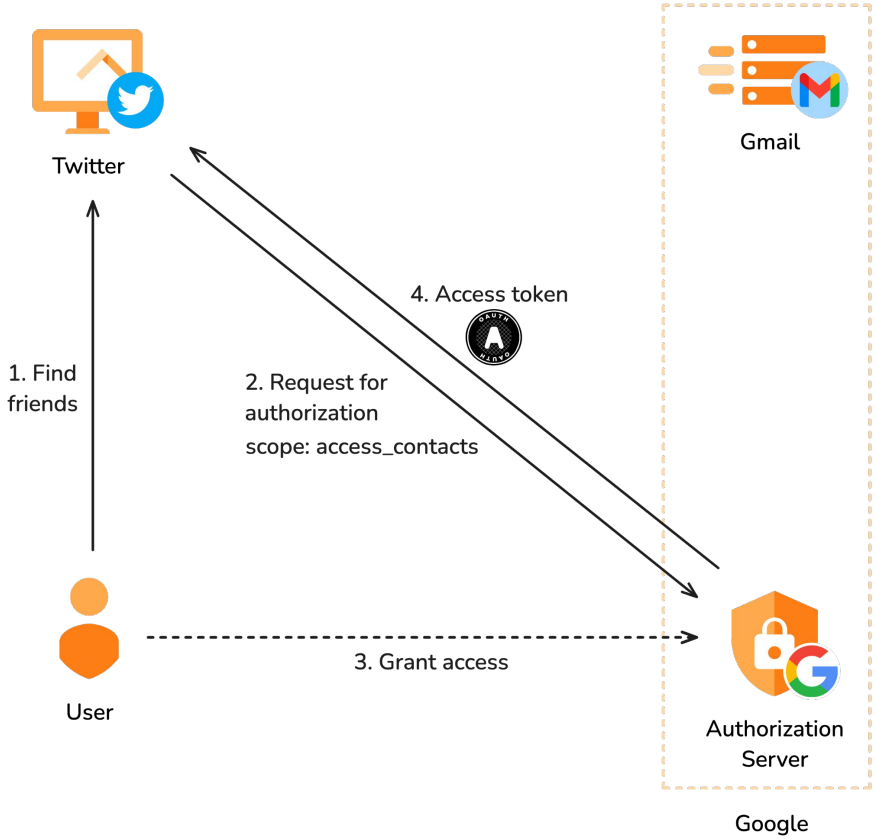
How OAuth Solved Credential Sharing: Access Delegation



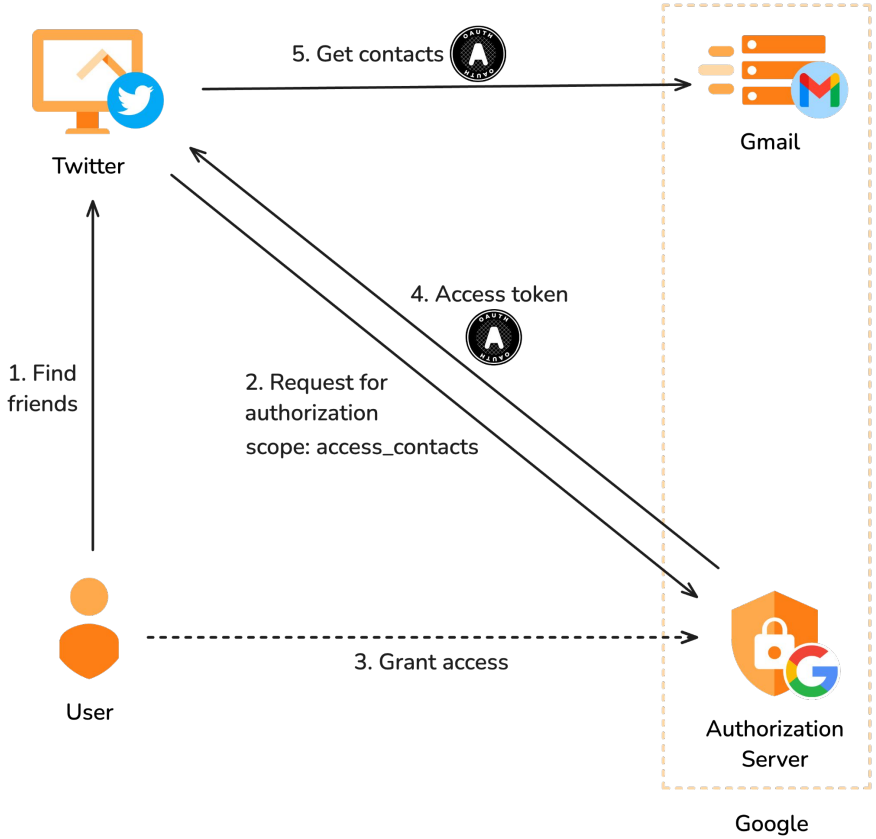
How OAuth Solved Credential Sharing: Access Delegation

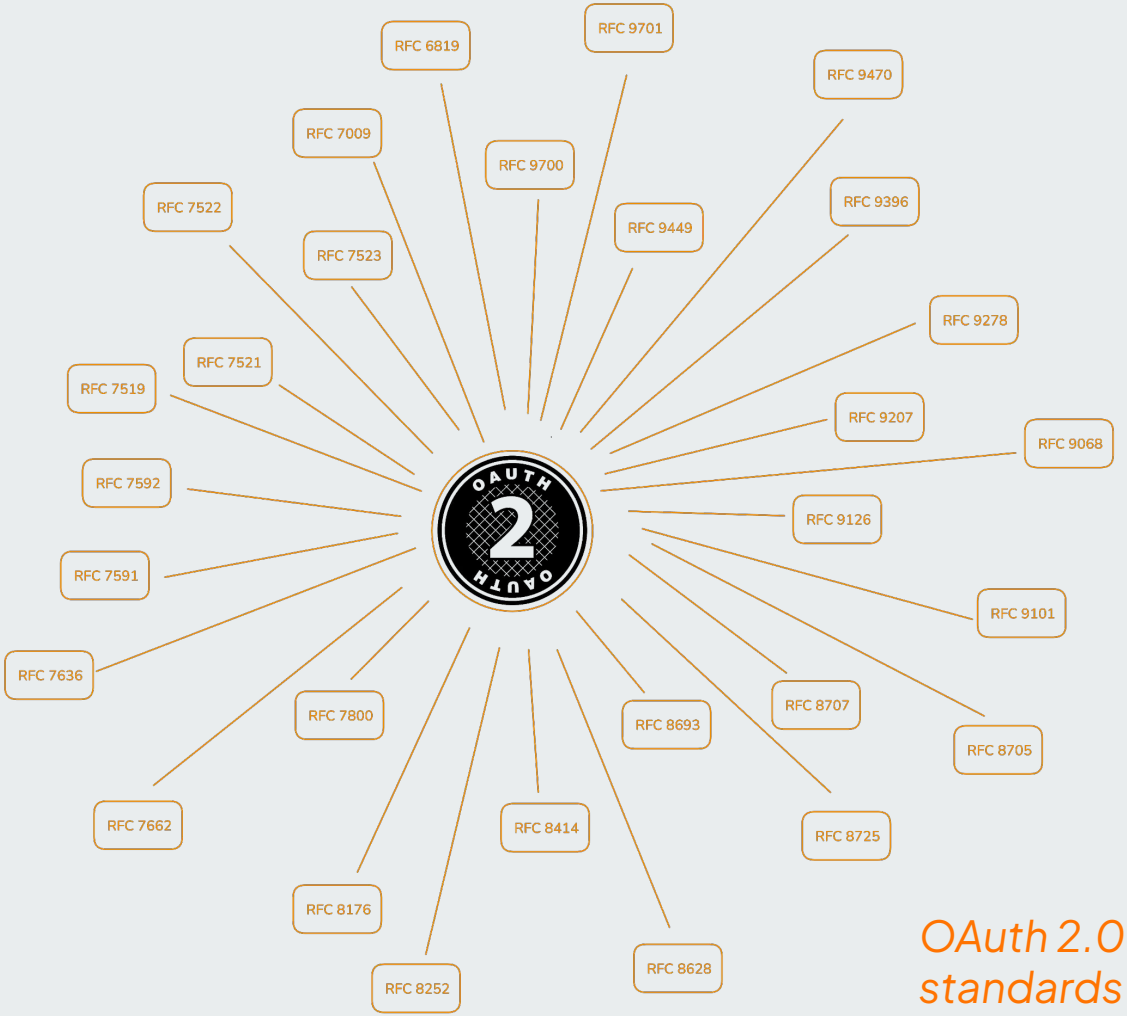


How OAuth Solved Credential Sharing: Access Delegation



How OAuth Solved Credential Sharing: Access Delegation

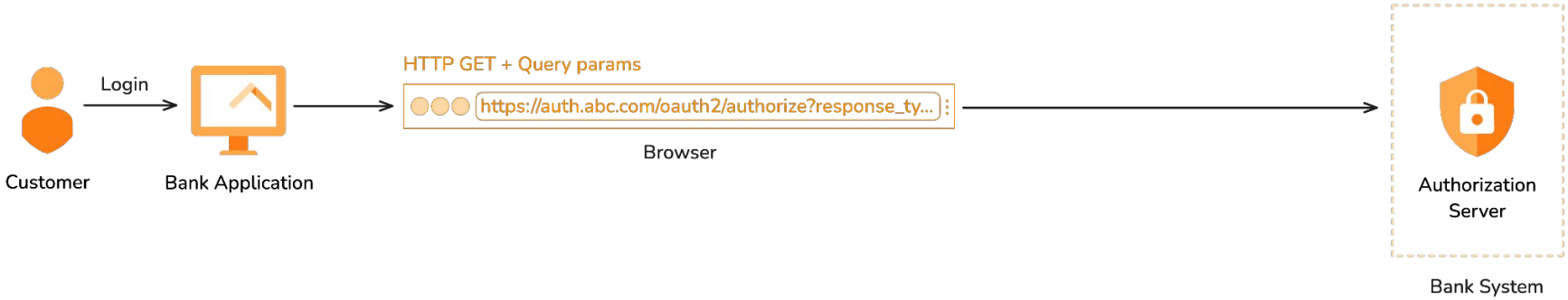




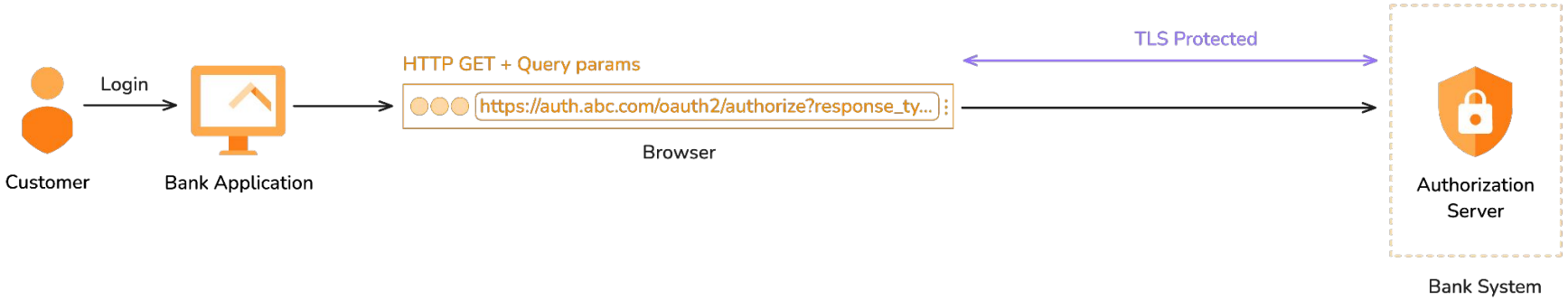
OAuth 2.0 related standards

Enhancing Privacy and Integrity Protection

Enhancing Privacy and Integrity Protection

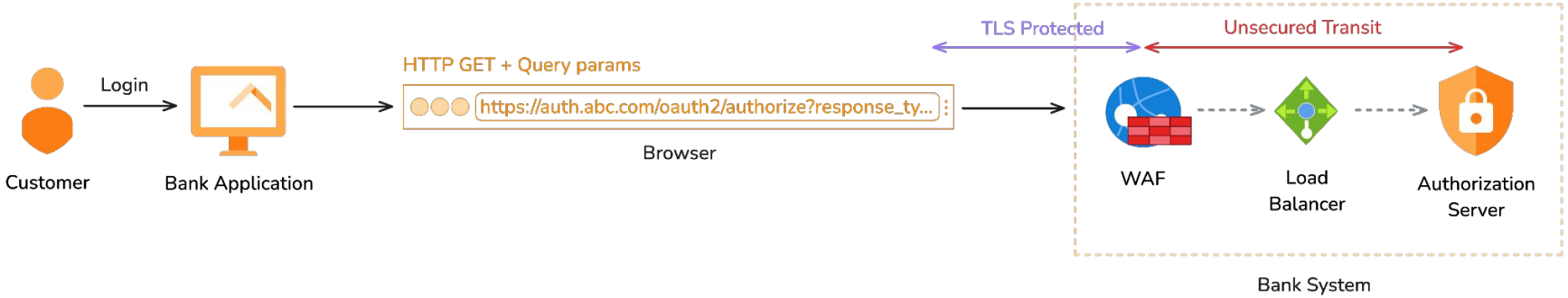


Enhancing Privacy and Integrity Protection

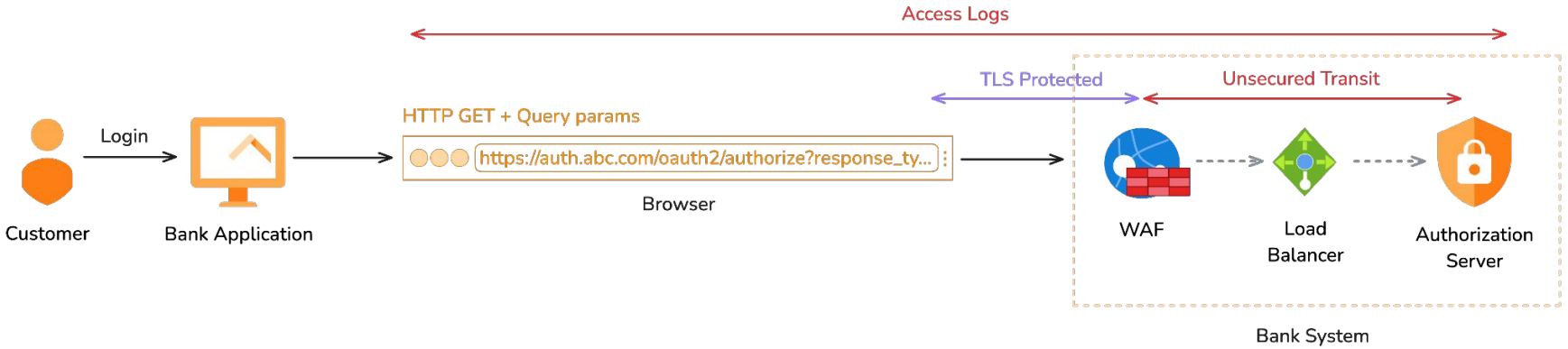


Enhancing Privacy and Integrity Protection

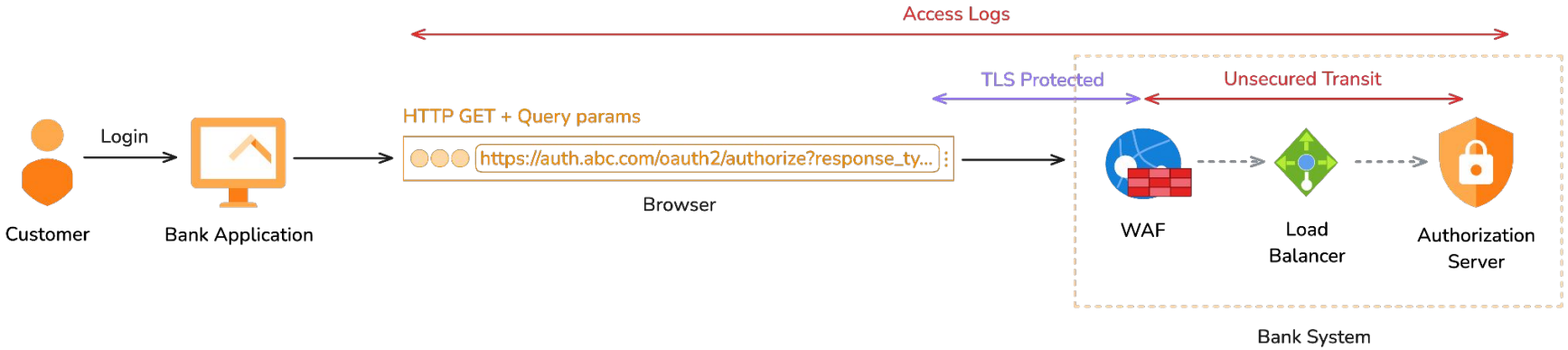
Enhancing Privacy and Integrity Protection



Enhancing Privacy and Integrity Protection

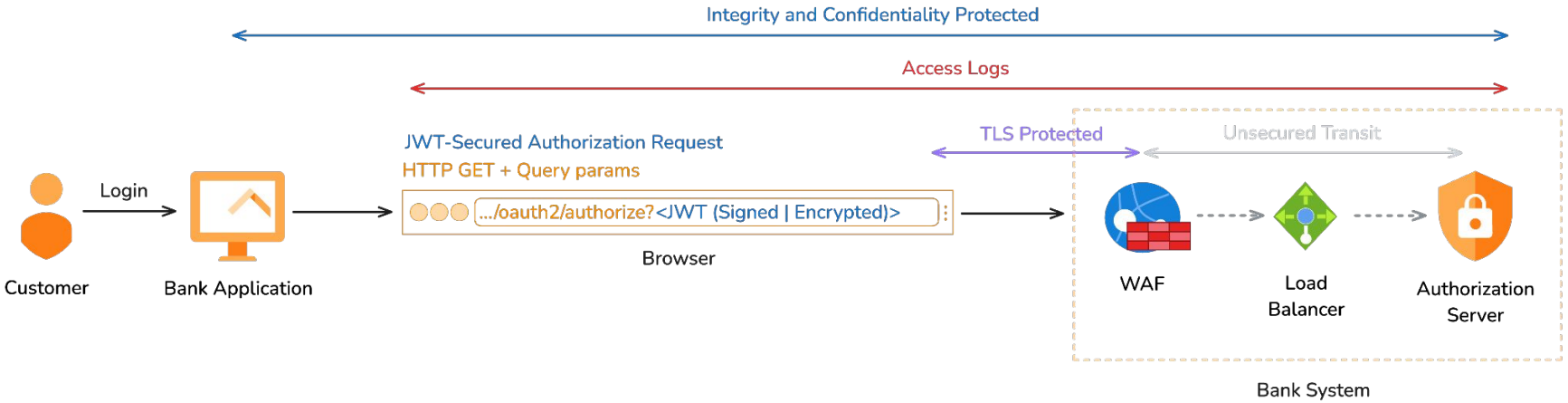


Enhancing Privacy and Integrity Protection



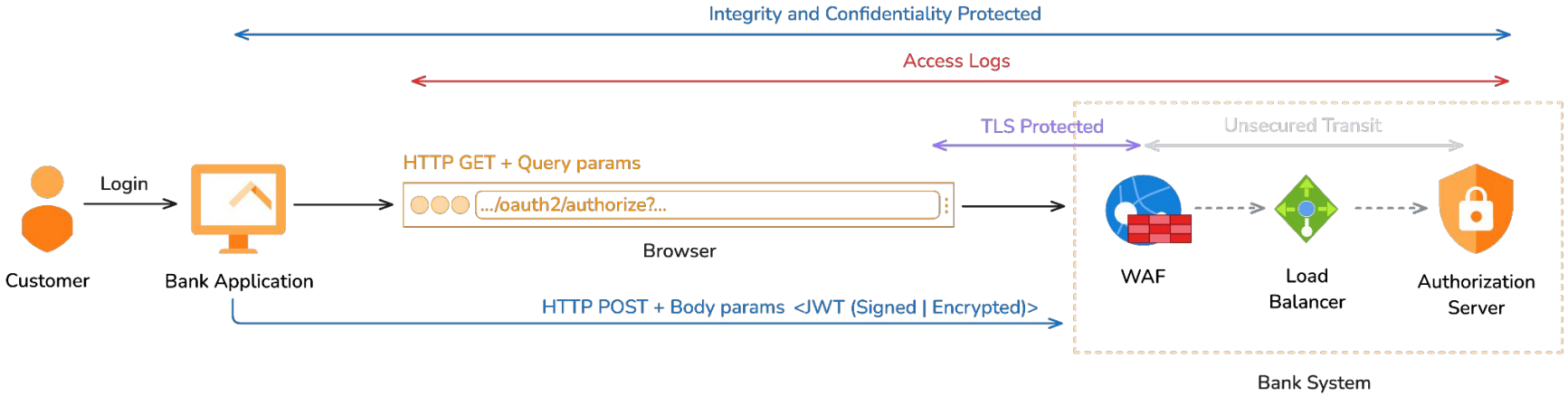
- Http GET request sent through browser with parameters in the URL
  - Data could be tampered with
  - Sensitive information gets logged at different levels
- Solutions from:
  - RFC 9101: The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request
  - RFC 9126: OAuth 2.0 Pushed Authorization Requests

Enhancing Privacy and Integrity Protection



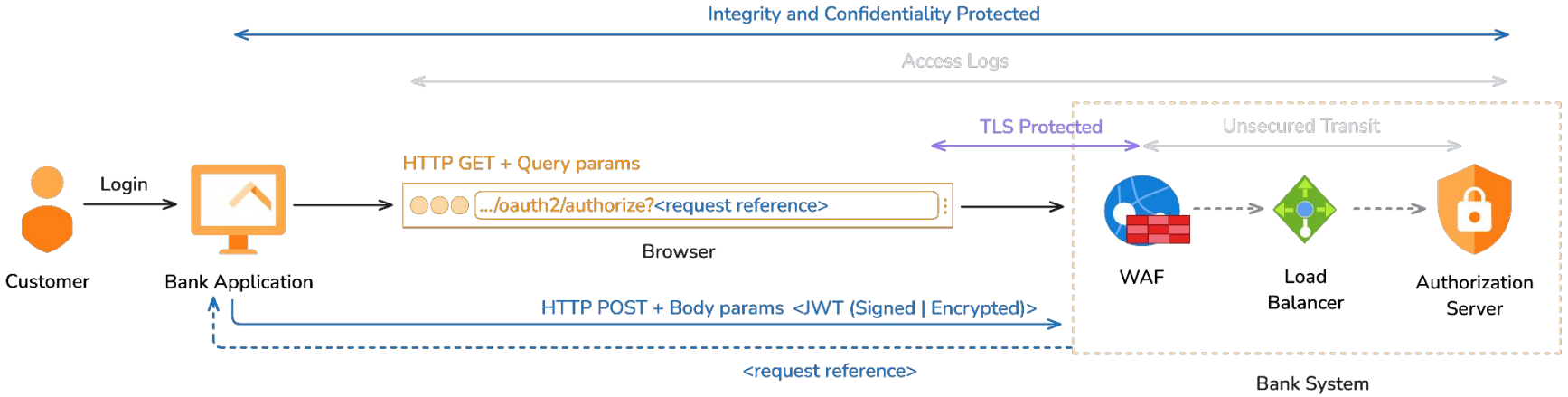
- RFC 9101: JWT-Secured Authorization Request

Enhancing Privacy and Integrity Protection



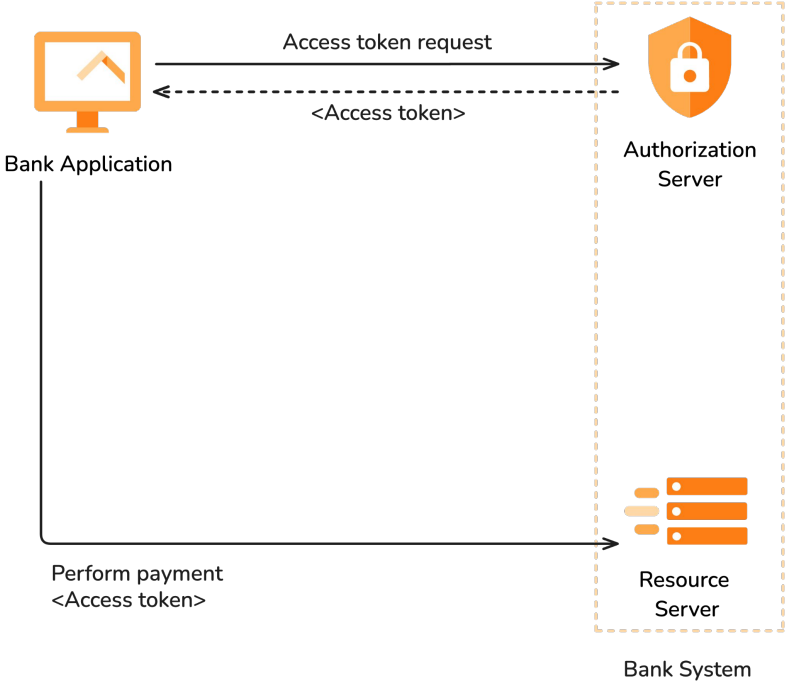
- RFC 9101: JWT-Secured Authorization Request
- RFC 9126: Pushed Authorization Requests

Enhancing Privacy and Integrity Protection



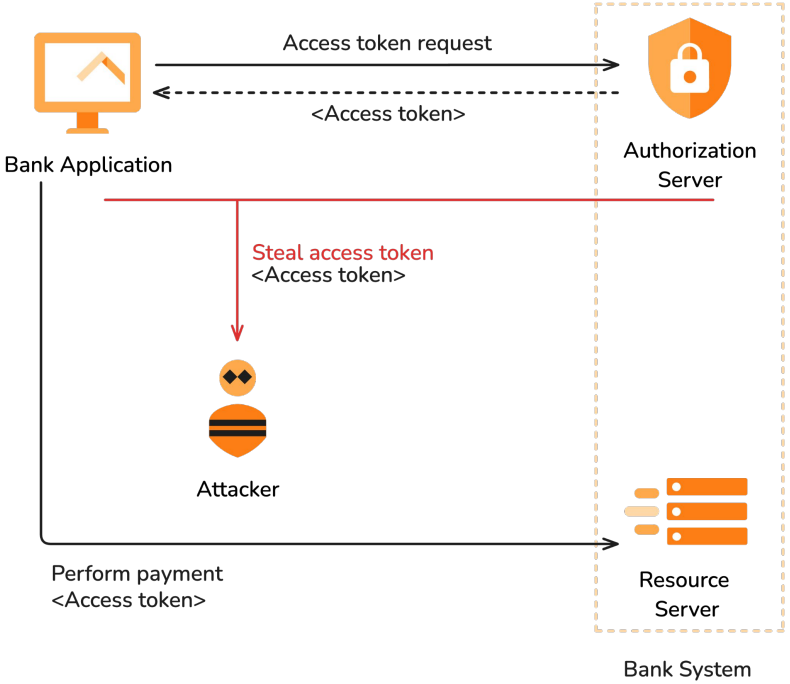
- RFC 9101: JWT-Secured Authorization Request
- RFC 9126: Pushed Authorization Requests

Securing Bearer Tokens



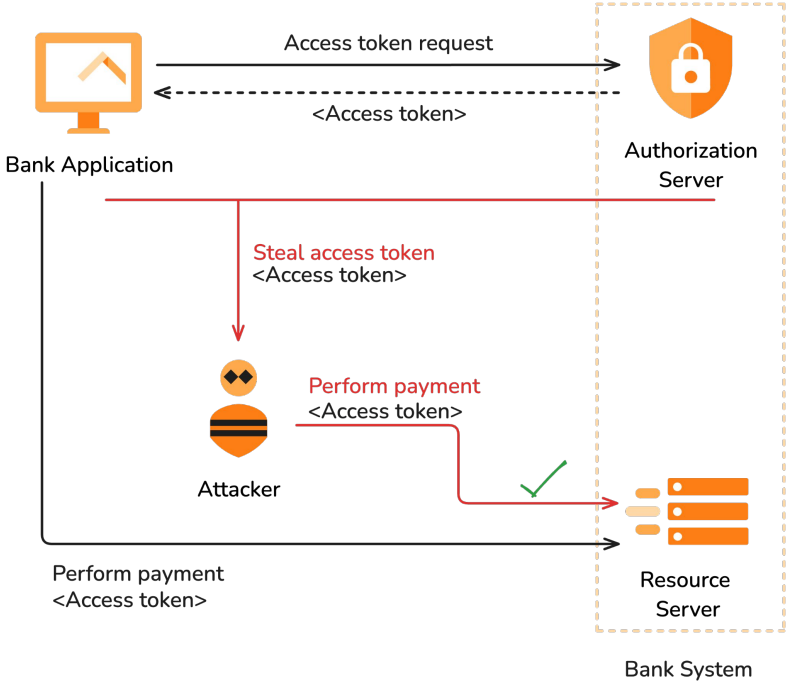
- Bearer tokens are like cash, if you have it you can use it

Securing Bearer Tokens



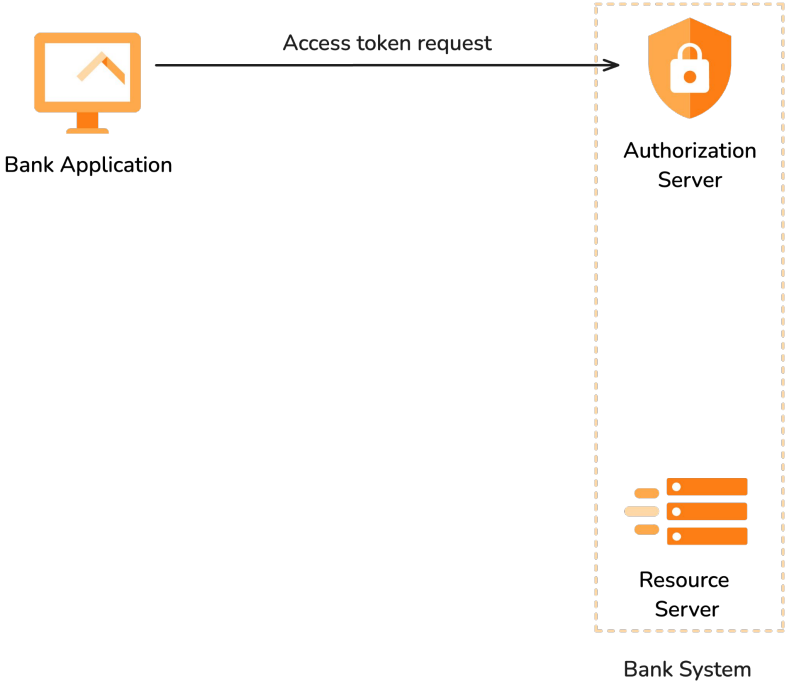
- Bearer tokens are like cash, if you have it you can use it

Securing Bearer Tokens



- Bearer tokens are like cash, if you have it you can use it

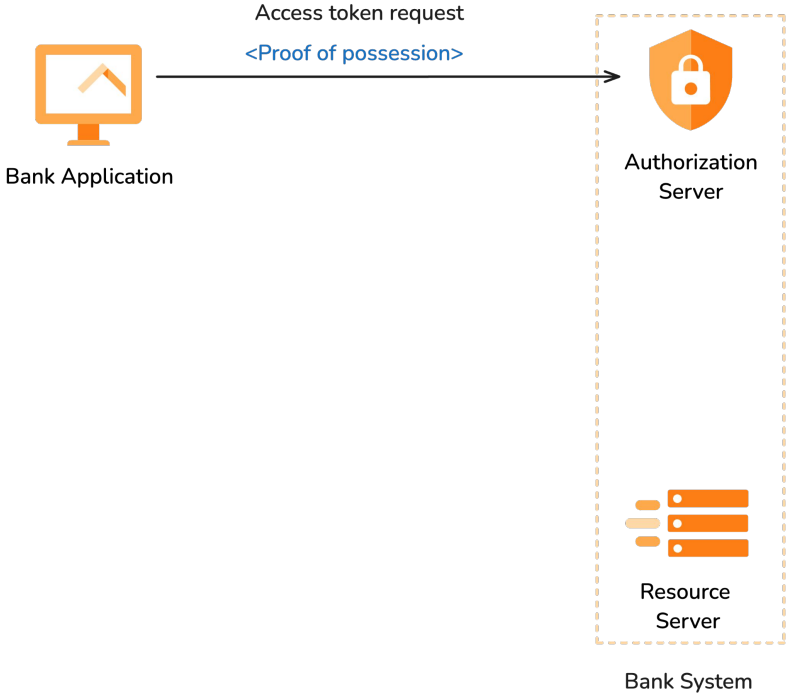
Securing Bearer Tokens



Solutions from:

- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 9449: OAuth 2.0 Demonstrating Proof of Possession

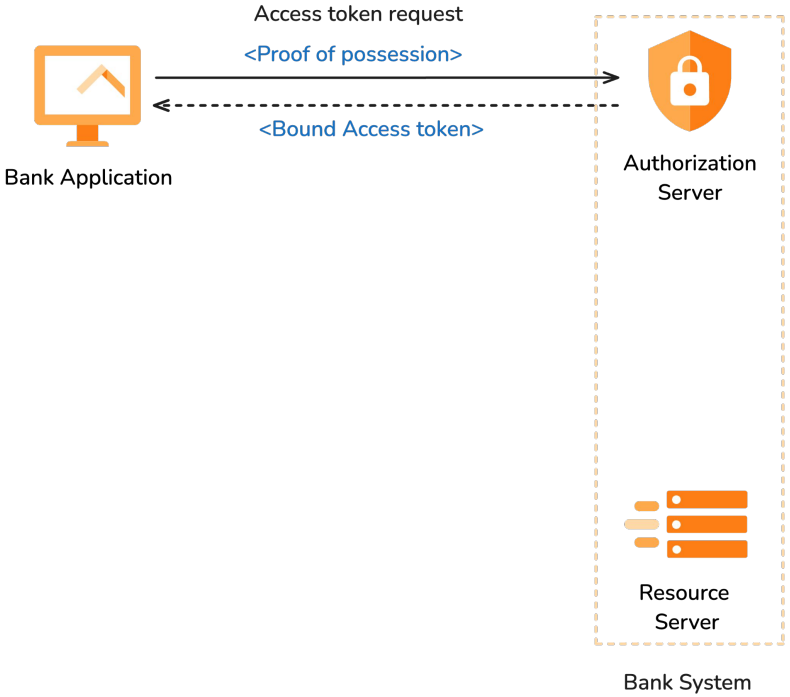
Securing Bearer Tokens



Solutions from:

- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 9449: OAuth 2.0 Demonstrating Proof of Possession

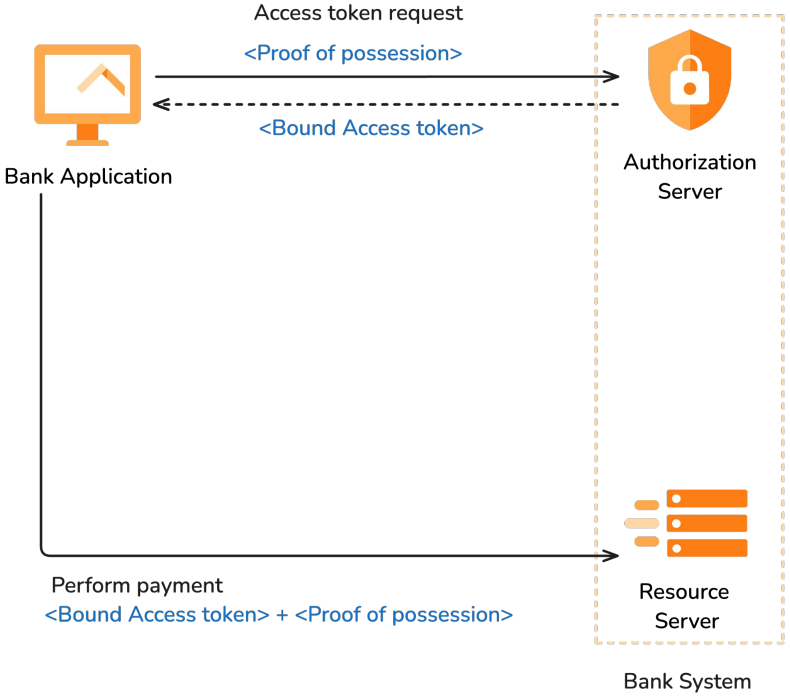
Securing Bearer Tokens



Solutions from:

- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 9449: OAuth 2.0 Demonstrating Proof of Possession

Securing Bearer Tokens

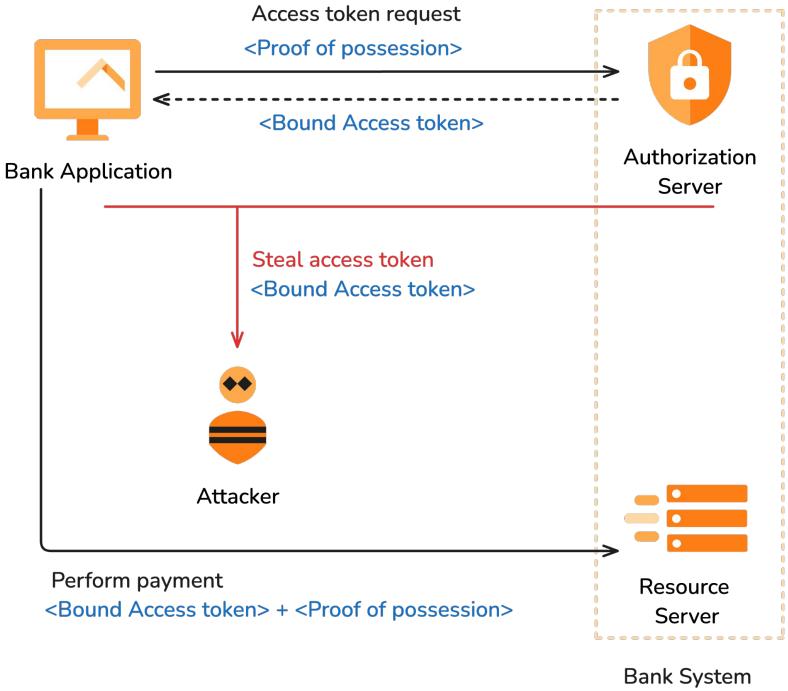


Solutions from:

- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 9449: OAuth 2.0 Demonstrating Proof of Possession

- Bound tokens are like a debit card with a PIN, you need both to use it

Securing Bearer Tokens

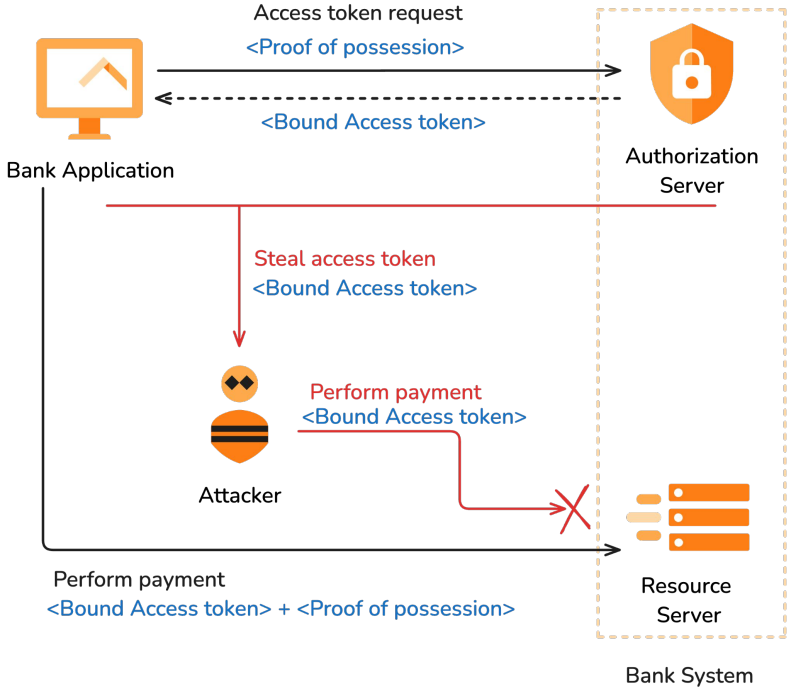


Solutions from:

- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 9449: OAuth 2.0 Demonstrating Proof of Possession

- Bound tokens are like a debit card with a PIN, you need both to use it

Securing Bearer Tokens



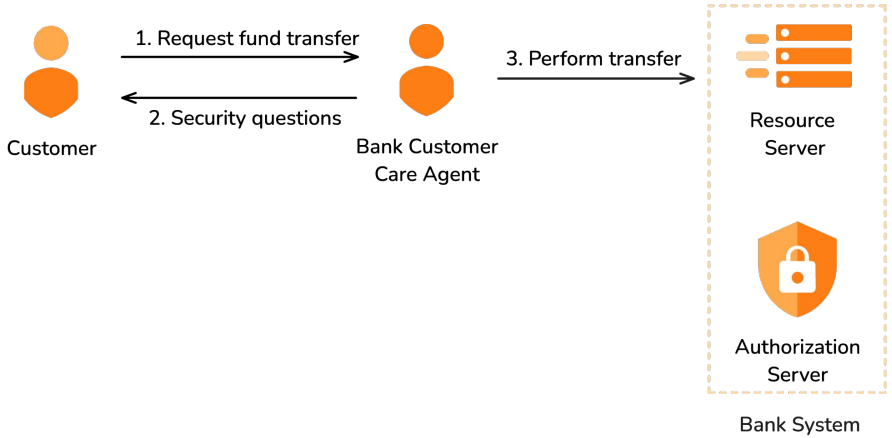
Solutions from:

- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 9449: OAuth 2.0 Demonstrating Proof of Possession

- Bound tokens are like a debit card with a PIN, you need both to use it

Decoupled Authentication

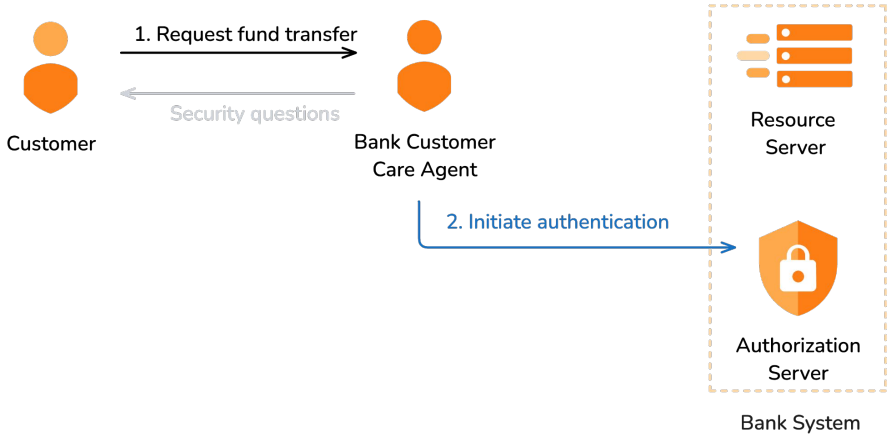
Doing a bank transaction via phone



- Stronger authentication?

Decoupled Authentication

Doing a bank transaction via phone



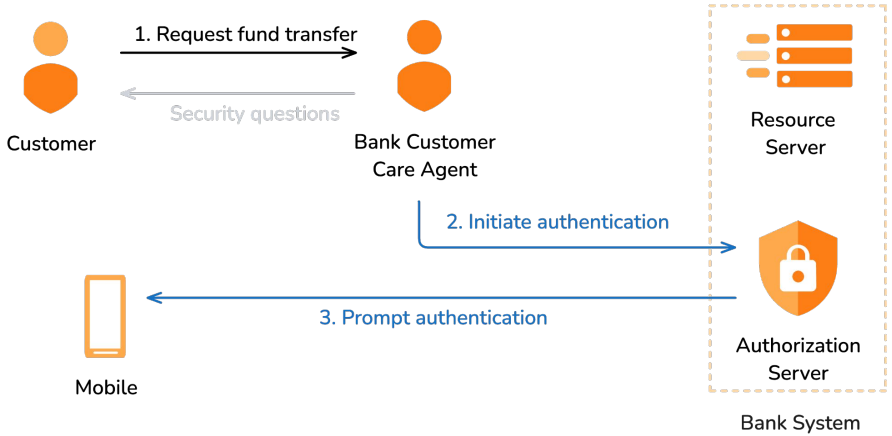
- Stronger authentication?

Solutions from:

- OpenID Connect Client-Initiated Backchannel Authentication Flow

Decoupled Authentication

Doing a bank transaction via phone



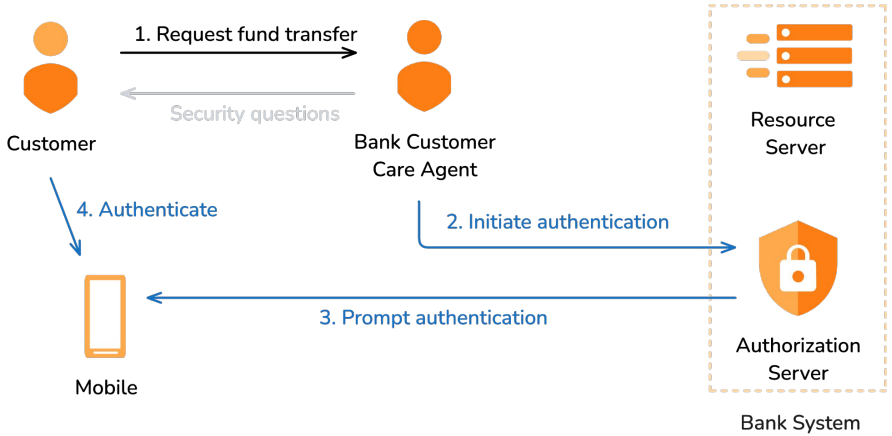
- Stronger authentication?

Solutions from:

- OpenID Connect Client-Initiated Backchannel Authentication Flow

Decoupled Authentication

Doing a bank transaction via phone



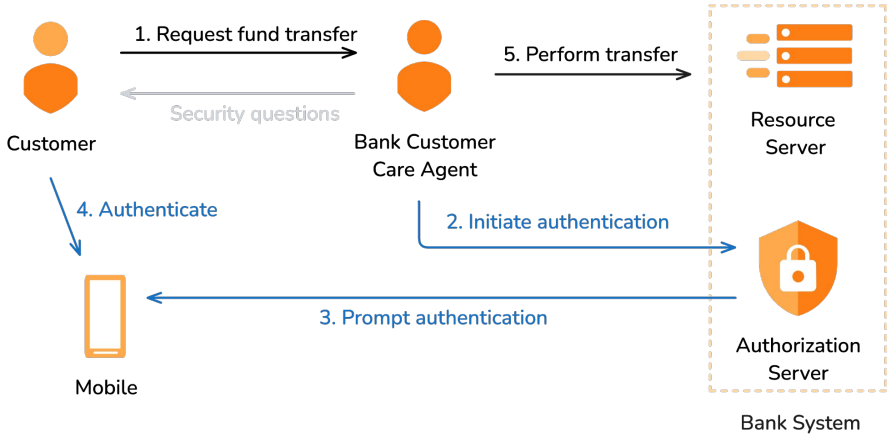
- Stronger authentication?

Solutions from:

- OpenID Connect Client-Initiated Backchannel Authentication Flow

Decoupled Authentication

Doing a bank transaction via phone

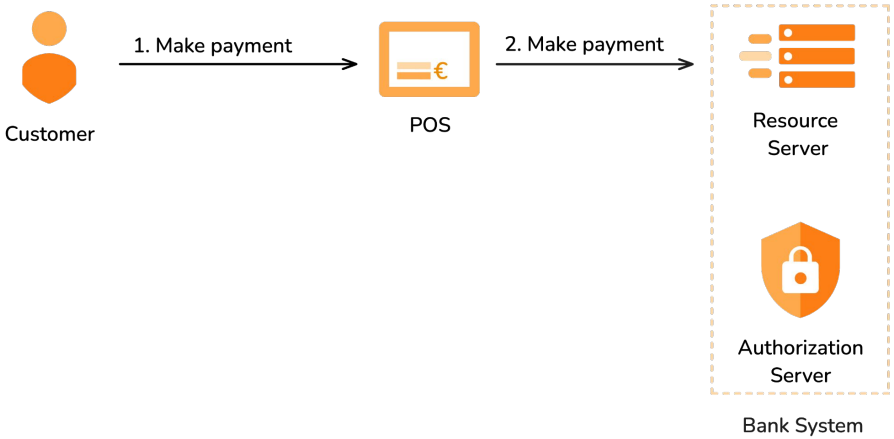


- Stronger authentication?

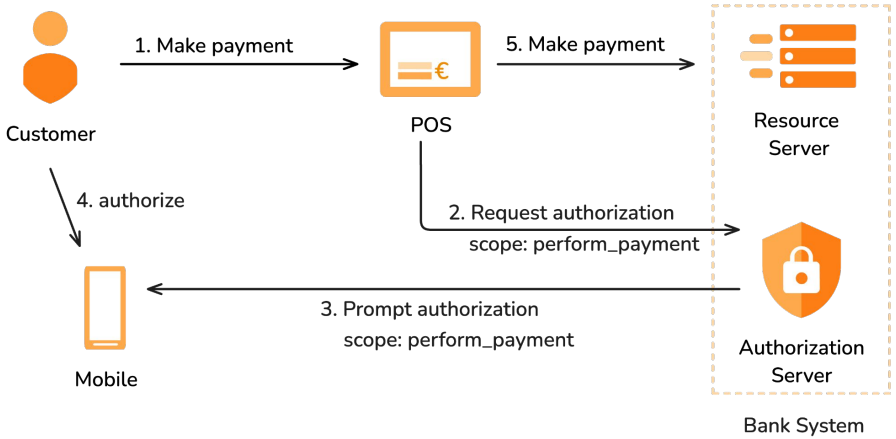
Solutions from:

- OpenID Connect Client-Initiated Backchannel Authentication Flow

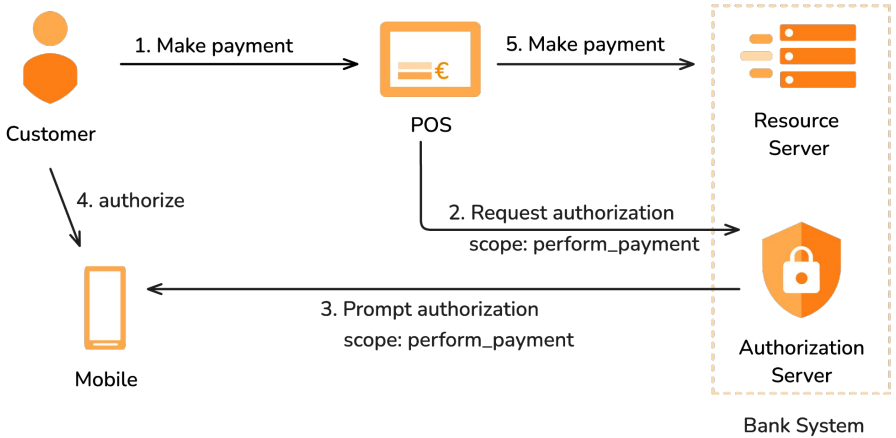
Fine-Grained Authorization Requests



Fine-Grained Authorization Requests

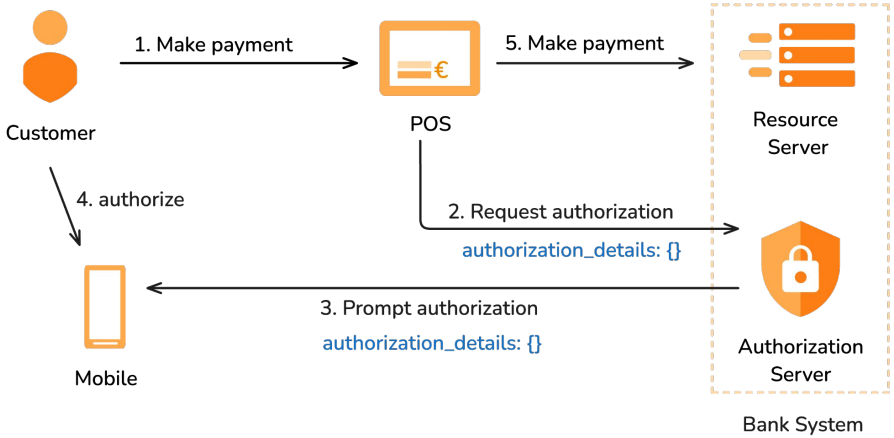


Fine-Grained Authorization Requests



- perform_payment → But how much?
- Coarse-grained authorization with scopes

Fine-Grained Authorization Requests



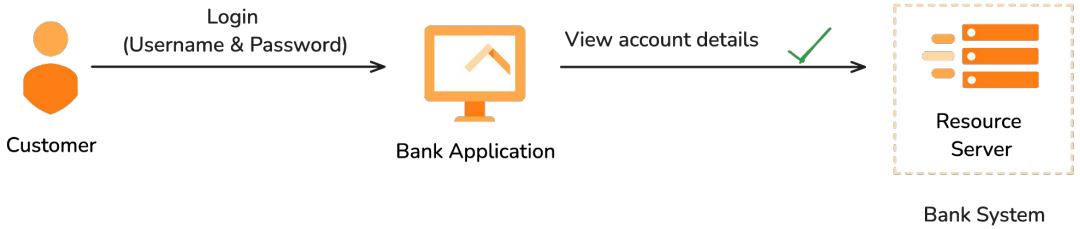
authorization_details

```
{
  "type": "payment_initiation"
  "instructedAmount": {
    "currency": "LKR",
    "amount": "123.50"
  },
  "creditorName": "Merchant A",
  "creditorAccount": {
    "bic":"ABCIDEFFXXX",
    "iban": "DE02100100109307118603"
  },
}
```

Solutions from:

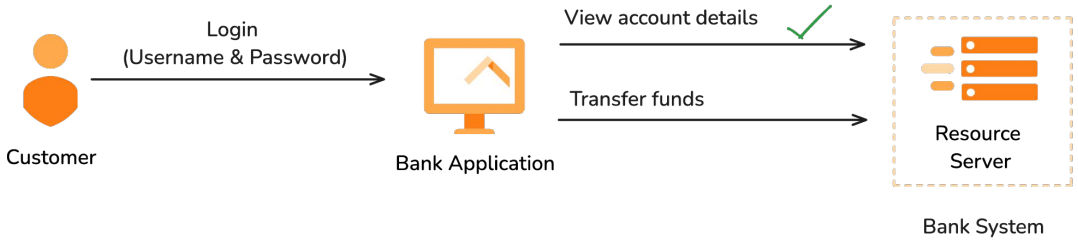
- RFC 9396: OAuth 2.0 Rich Authorization Requests

Performing actions that require a higher assurance level



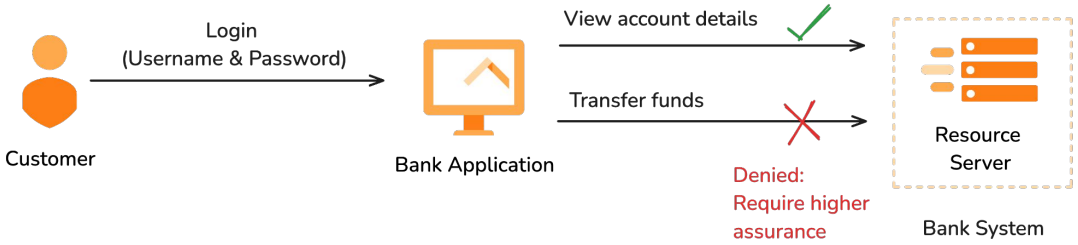
- **View account details** require authentication with **username & password**

Performing actions that require a higher assurance level



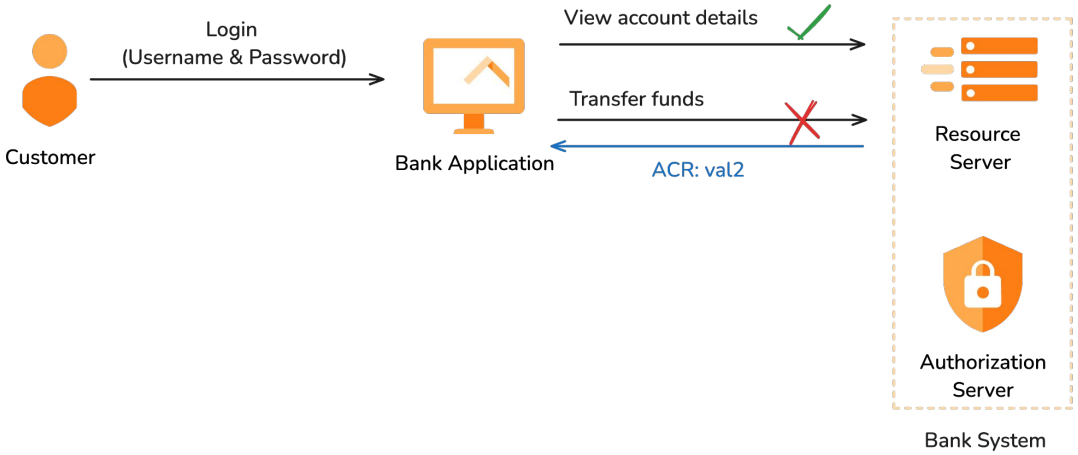
- **View account details** require authentication with **username & password**
  - Is this enough for a fund transfer?

Performing actions that require a higher assurance level



- **View account details** require authentication with **username & password**
  - Is this enough for a fund transfer?
- **Transfer funds** require authentication with **username & password** and **OTP**

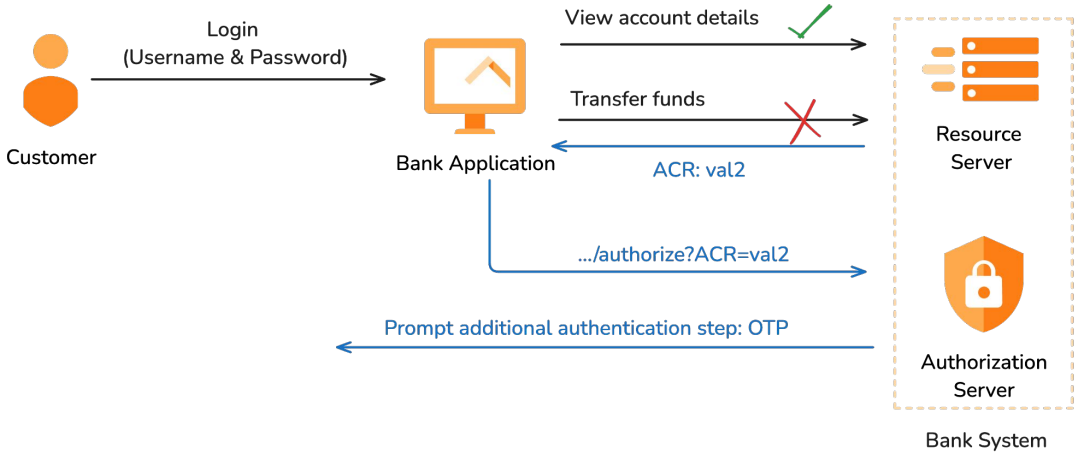
Performing actions that require a higher assurance level



Solutions from:

- RFC 9470: OAuth 2.0 Step Up Authentication Challenge Protocol

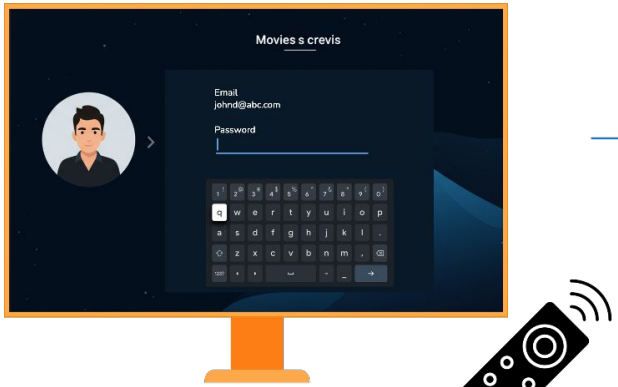
Performing actions that require a higher assurance level



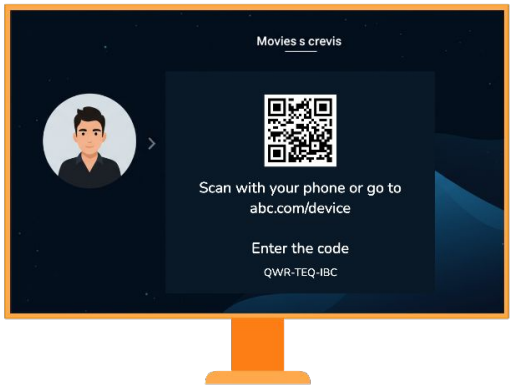
Solutions from:

- RFC 9470: OAuth 2.0 Step Up Authentication Challenge Protocol

Authorization for Input Constrained Devices



Smart TV App Login



Smart TV App Login
with
Device Authorization Grant

- Hindered authentication experience

Solutions from:

- RFC 8628: OAuth 2.0 Device Authorization Grant

Authorization for Browserless Devices

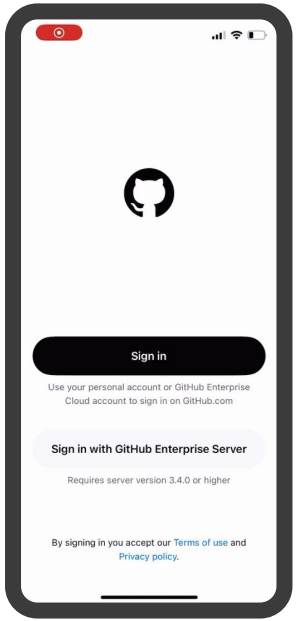
```
Last login: Mon Jul 21 17:20:36 on ttys012
janak@192 ~ % az login --use-device-code
To sign in, use a web browser to open the page https://microsoft.com/devicelogin
 and enter the code N9HD5PE36 to authenticate.
```

- Strong authentication?
- What if there is no input capability at all?

Solutions from:

- RFC 8628: OAuth 2.0 Device Authorization Grant

Enhancing UX for First-Party Applications



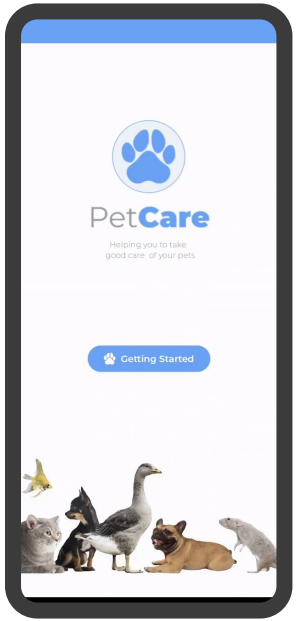
GitHub mobile app for iOS

- Disconnected experience with browser redirection

Why not Password Grant?

- Only password based logins
- No options for MFA and social logins

Enhancing UX for First-Party Applications



UX with OAuth 2.0 for
First-Party Applications

Solutions from:

- DRAFT: OAuth 2.0 for First-Party Applications

Best Current Practice Documents

- RFC 8252: OAuth 2.0 for Native Apps
  - Published in 2017
- RFC 8725: JSON Web Token Best Current Practices
  - Published in 2020
  - Revisions are on the works
- RFC 9700: Best Current Practice for OAuth 2.0 Security
  - Published in 2025
- DRAFT: Cross-Device Flows: Security Best Current Practice
- DRAFT: OAuth 2.0 for Browser-Based Applications

OAuth 2.1: A Modernized OAuth

- OAuth 2.0 was published in 2012 – over 13 years ago!
  - Security needs evolved, and additional standards emerged

- What is OAuth 2.1?
  - A streamlined update to OAuth 2.0
  - **Nothing new**, just consolidates best practices
  - Removes outdated flows for better security

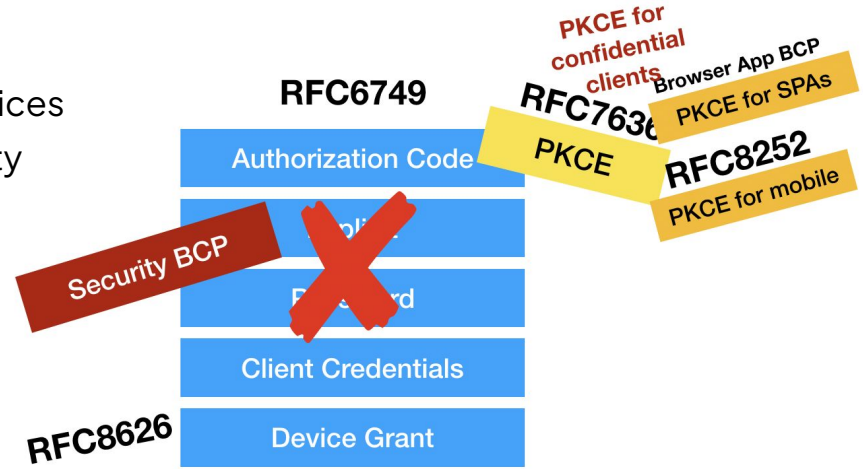


Image src:
https://aaronparecki.com/2019/12/12/21/its-time-for-oauth-2-dot-1

What About Standards for AI Agent Use Cases?

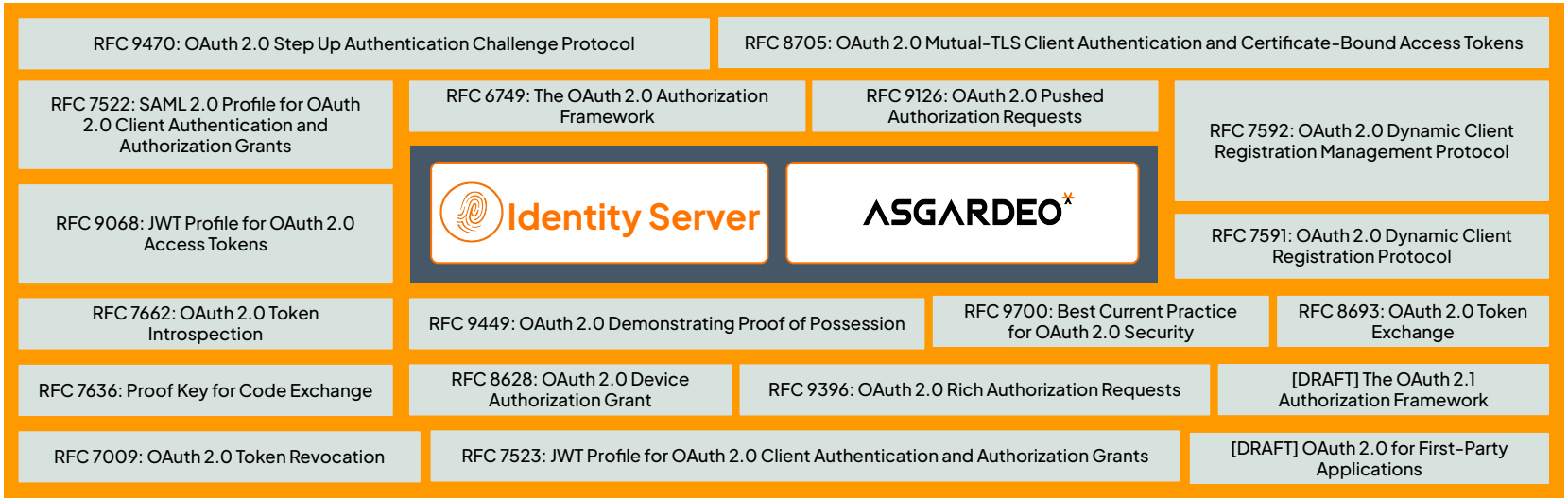
- Still at early stage discussions in the communities
  - Reusing existing standards where appropriate
  - Developing new standards where needed

Secure Your AI with IAM for Agents
Ayesha Dissanayaka
Associate Director & Architect, WSO2
04:00 p.m.

Why Standards Matter

- Interoperability
  - Enables independent systems to securely communicate using a common protocol
- No vendor lock-in
  - Built on shared protocols, not proprietary APIs
- Rigorously reviewed by identity experts

Supported and Upcoming OAuth Standards in WSO2 IAM Platform



** Supported and upcoming OpenId Foundation specifications are not listed here.*


Thank you!
20TH ANNIVERSARY EDITION
WSO2CONASIA
PLATFORMLESS MODERNIZATION