Getting Started with OAuth 2.0

API SECURITY 101

Scott Brady
IDENTITY & ACCESS CONTROL LEAD

@scottbrady91 www.scottbrady91.com

Overview

The problem of API authorization

Previous solutions

OAuth 2.0

OAuth 2.0 misunderstandings

Things Used to be a Little Different

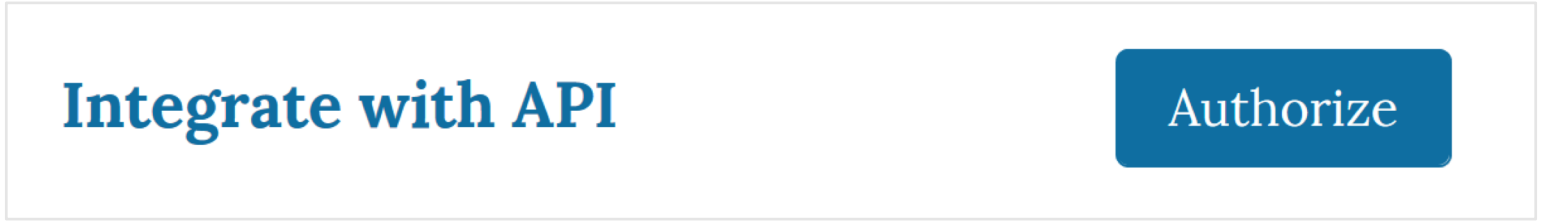
Past	Present
XML	JSON
SOAP	HTTP APIs
SAML or WS-*	OAuth & OpenID Connect

Vocabulary

Authentication

Authorization

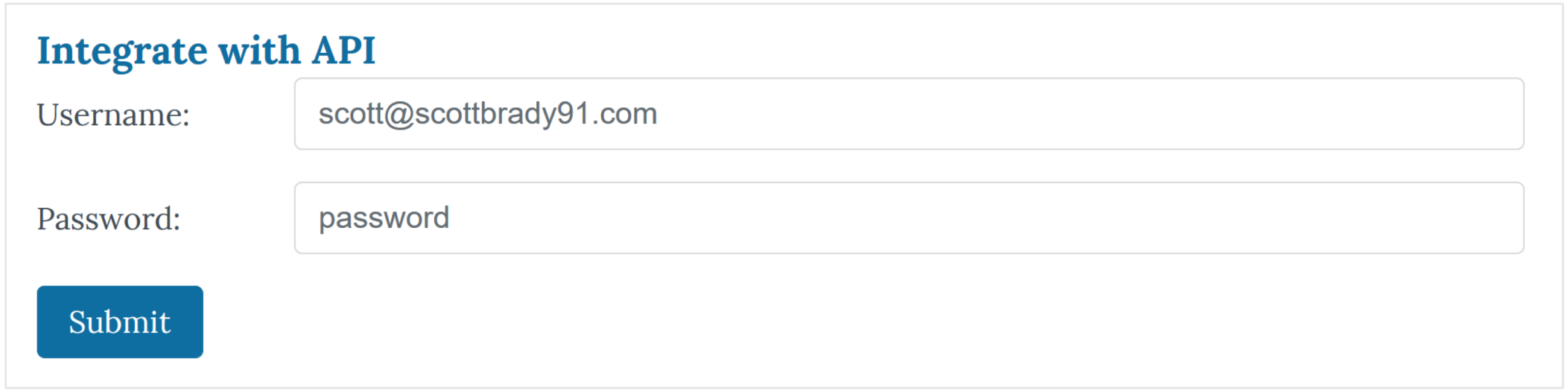
The Problem of API Authorization



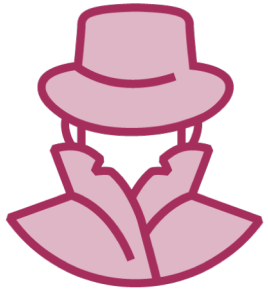
Allow an application to access an API to send an email on a user's behalf

A Solution: Credential Sharing

Credential Sharing



The Problems with Credential Sharing



Impersonation

Revocation

Exposed user credentials

Something you know

Federation

Incompatibilities

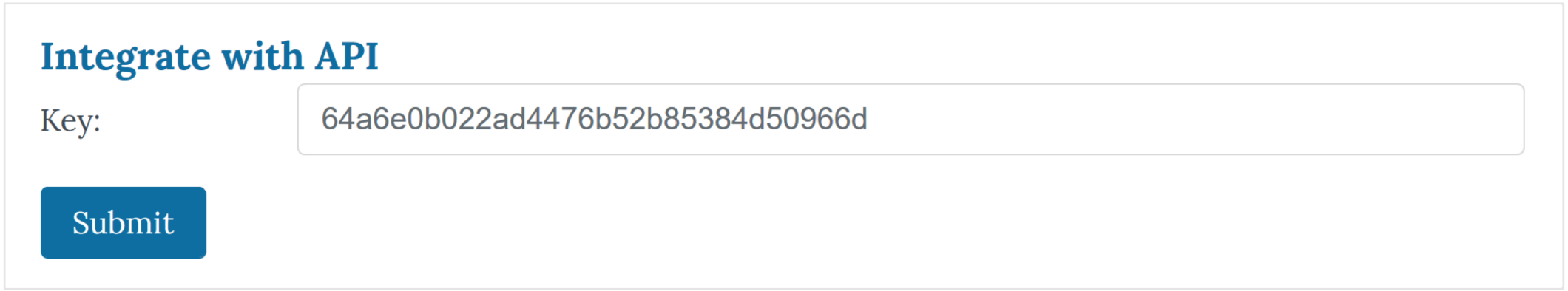
A Solution: Cookies

A Solution: Cookies

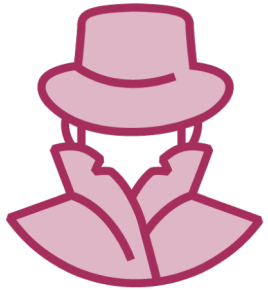
Cross-Site Request Forgery (CSRF, aka XSRF)

A Solution: API Keys

A Solution: API Keys



API Keys



Impersonation

Revocation

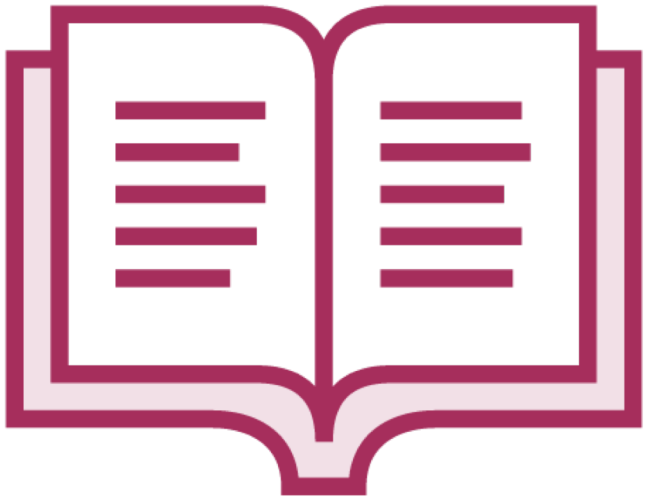
Exposed user credentials

Something you know

Federation

Incompatibilities

API Key Limitations



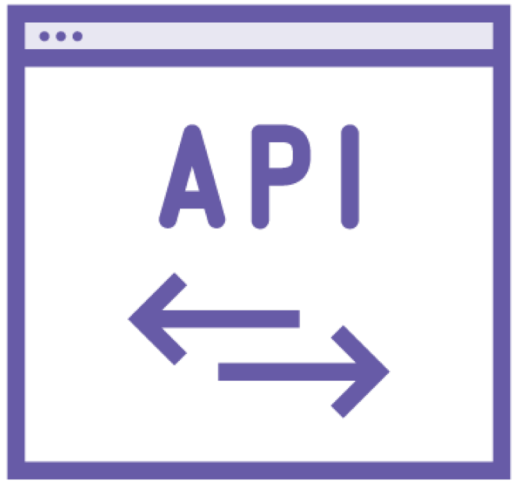
No standards

Expiration

The Solution: OAuth 2.0

OAuth 2.0

Authorization framework

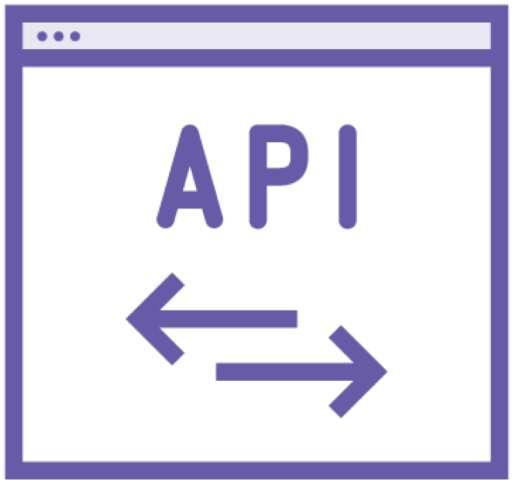


Built for HTTP APIs

Scoped access

Delegation protocol

The OAuth 2.0 Players



Protected Resource (HTTP API)

Client (requesting application)

Resource Owner (the user)

Authorization Server

The OAuth Dance

Resource Owner

Authentication & Consent

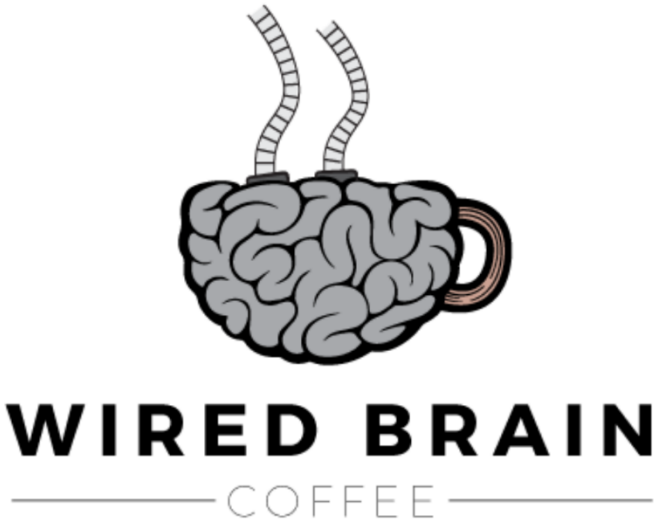
Authorization Server

Authorization Request

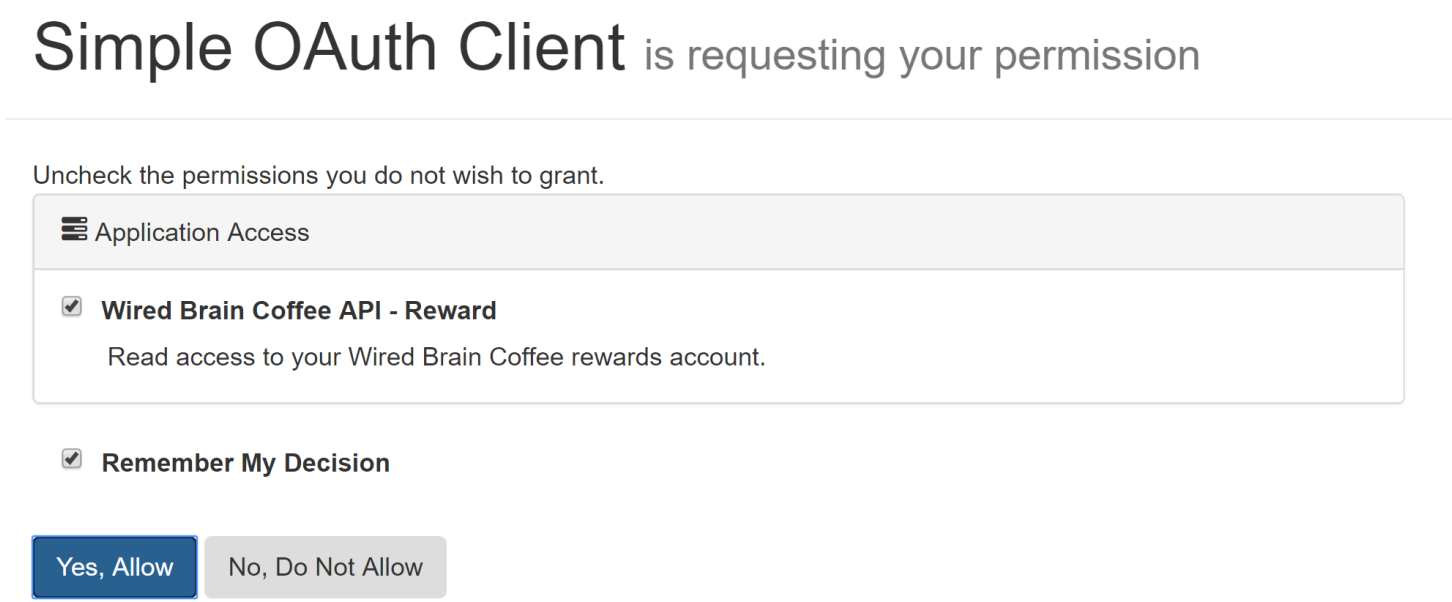
Client Application

Protected Resource

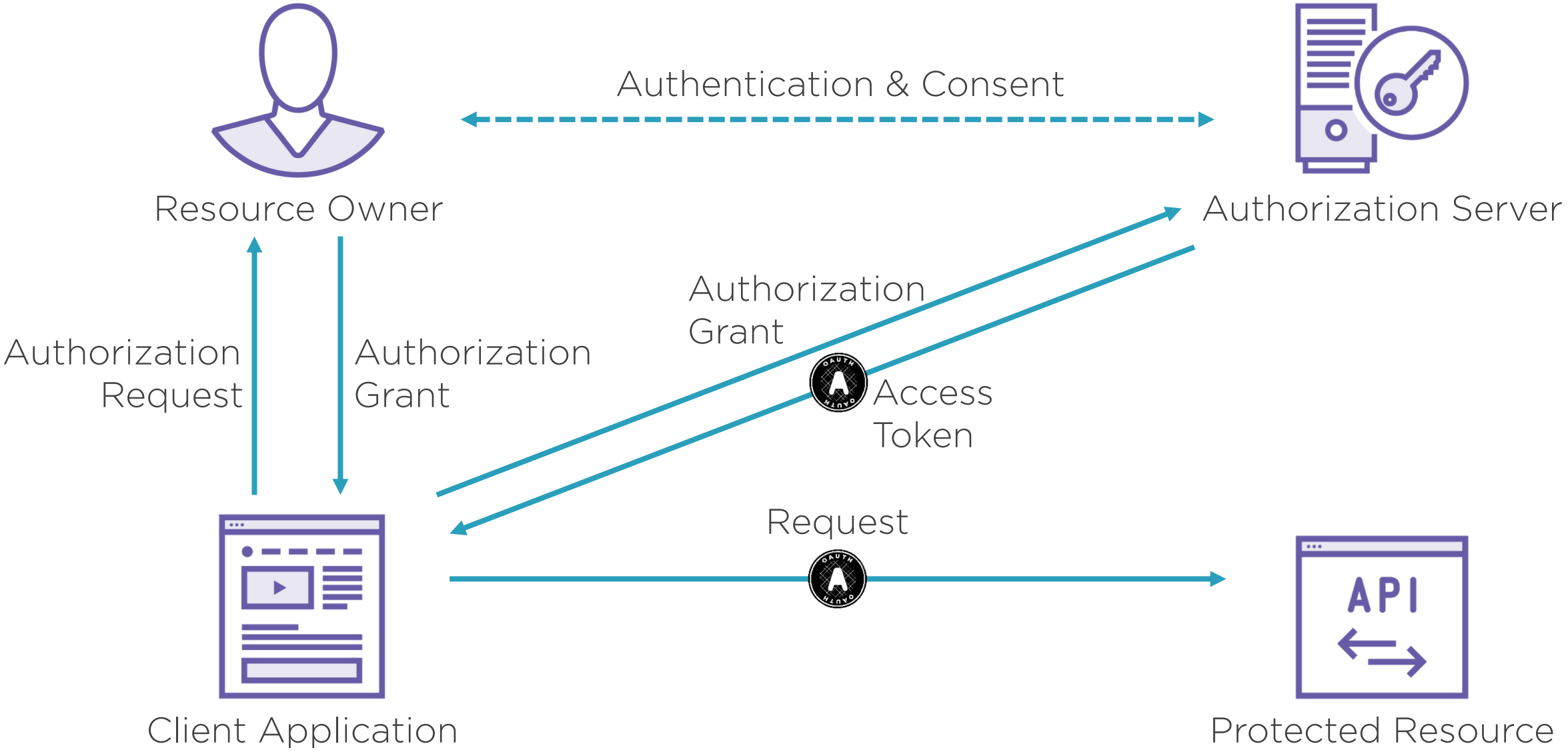
Authorization Server: User Authentication



Authorization Server: User Consent



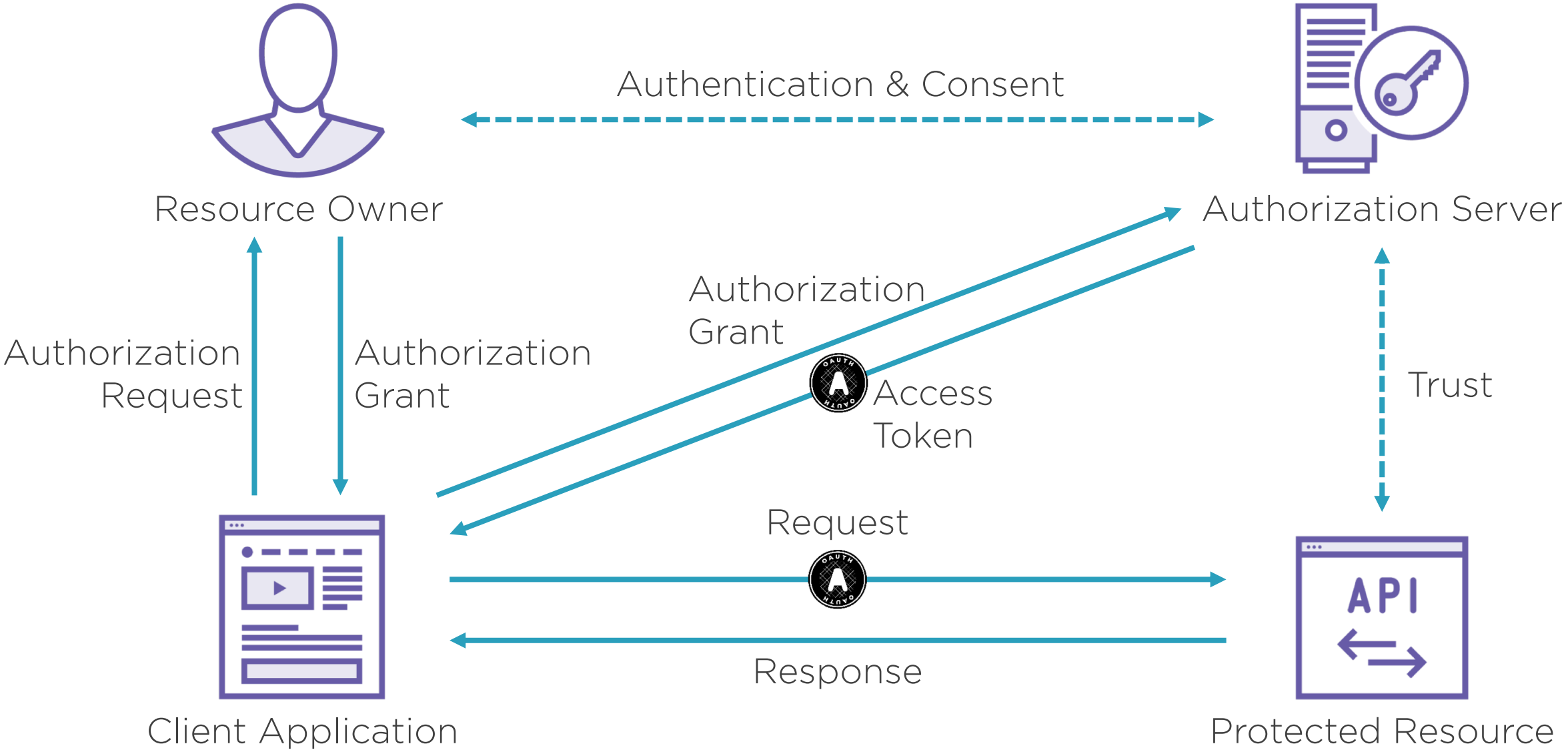
The OAuth Dance



OAuth Access Token Usage

```
Authorization: Bearer f4ht3qqw80by4d28aa7384oenx2f8pqo
```

The OAuth Dance



Demo

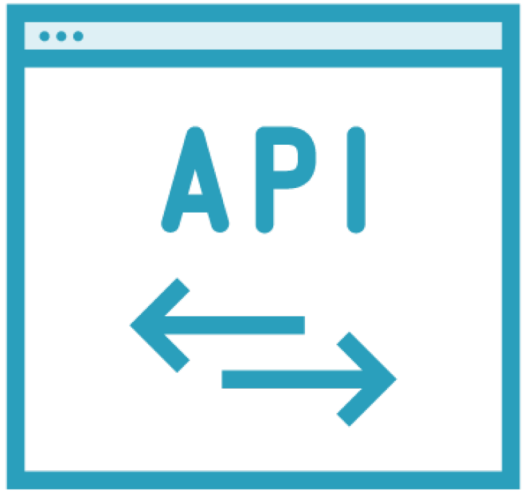
A typical OAuth 2.0 authorization request

OAuth: A Misunderstood Protocol

Authentication Confusion

OAuth != Authentication

Access tokens do not represent the user



The client is not the token's intended audience

Client cannot reliably verify the token

Too Abstract

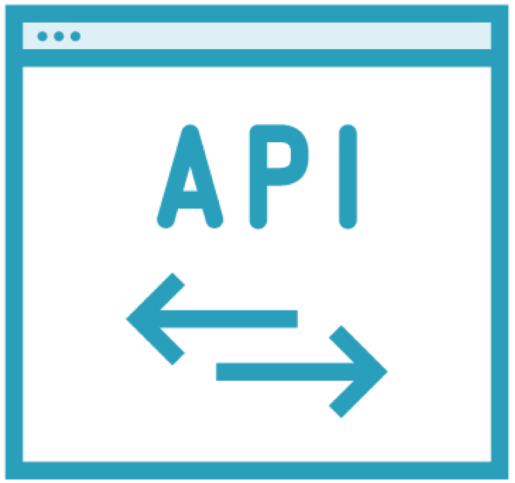
Access token format

Access token validation

User authentication

What OAuth Got *Very* Right

Delegated access



API access control

Separation of user & client credentials

User consent

OAuth 2.0 is a framework

Summary

The problem of API authorization

Previous solutions

OAuth 2.0

OAuth 2.0 misunderstandings