



The API Gatekeeper

Dick Hardt

The Apigee logo, consisting of the word 'apigee' in white lowercase letters on an orange rectangular background. The background of the slide features a faint, light gray line-art illustration of a city skyline with several suspension bridges, including the Golden Gate Bridge, and various skyscrapers.

apigee

Agenda



Agenda



- Access Control Overview

Agenda



- Access Control Overview
- OAuth History

Agenda



- Access Control Overview
- OAuth History
- OAuth Flows

Agenda



- Access Control Overview
- OAuth History
- OAuth Flows
- Implementation Steps

Agenda



- Access Control Overview
- OAuth History
- OAuth Flows
- Implementation Steps
- What can go wrong?

Agenda



- Access Control Overview
- OAuth History
- OAuth Flows
- Implementation Steps
- What can go wrong?
- Q & A

Authorization Code



Authorization Code

- key into database

Authorization Code

- key into database
 - user, scope, app id, expiry (5 min)

Authorization Code

- key into database
 - user, scope, app id, expiry (5 min)
- token (self contained)

Authorization Code

- key into database
 - user, scope, app id, expiry (5 min)
- token (self contained)
 - user, scope, app id, expiry (5 min)

Authorization Code

- key into database
 - user, scope, app id, expiry (5 min)
- token (self contained)
 - user, scope, app id, expiry (5 min)
 - JWT

Access Token Lifecycle



Access Token Lifecycle

- key into database

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status
- token (self contained)

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status
- token (self contained)
 - user, scope, app id, expiry (60 minutes)

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status
- token (self contained)
 - user, scope, app id, expiry (60 minutes)
 - JWT

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status
- token (self contained)
 - user, scope, app id, expiry (60 minutes)
 - JWT
- Refresh token

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status
- token (self contained)
 - user, scope, app id, expiry (60 minutes)
 - JWT
- Refresh token
 - user, scope, app id, expiry / status

Access Token Lifecycle

- key into database
 - user, scope, app id, expiry, status
- token (self contained)
 - user, scope, app id, expiry (60 minutes)
 - JWT
- Refresh token
 - user, scope, app id, expiry / status
 - JWT

API Authorization Middleware

implementation dependent

X-RateLimit-Limit: 500

X-RateLimit-Remaining: 432

Developer Documentation / Sandbox

Developer Documentation / Sandbox



What can go wrong?



What can go wrong?

- Compromise of client secret

What can go wrong?

- Compromise of client secret
- Compromise of access tokens (server)

What can go wrong?

- Compromise of client secret
- Compromise of access tokens (server)
 - Developer rests client secret

What can go wrong?

- Compromise of client secret
- Compromise of access tokens (server)
 - Developer rests client secret
 - All access tokens are invalidated

What can go wrong?

- Compromise of client secret
- Compromise of access tokens (server)
 - Developer rests client secret
 - All access tokens are invalidated
 - Refresh tokens still work, but require new secret

What can go wrong?

- Compromise of client secret
 - Developer rests client secret
 - All access tokens are invalidated
 - Refresh tokens still work, but require new secret
- Compromise of access token (client)

What can go wrong?

- Compromise of client secret
- Compromise of access tokens (server)
 - Developer rests client secret
 - All access tokens are invalidated
 - Refresh tokens still work, but require new secret
- Compromise of access token (client)
 - User revokes authorization

What can go wrong?

- Compromise of client secret
- Compromise of access tokens (server)
 - Developer rests client secret
 - All access tokens are invalidated
 - Refresh tokens still work, but require new secret
- Compromise of access token (client)
 - User revokes authorization
- ***Resolution is self service***