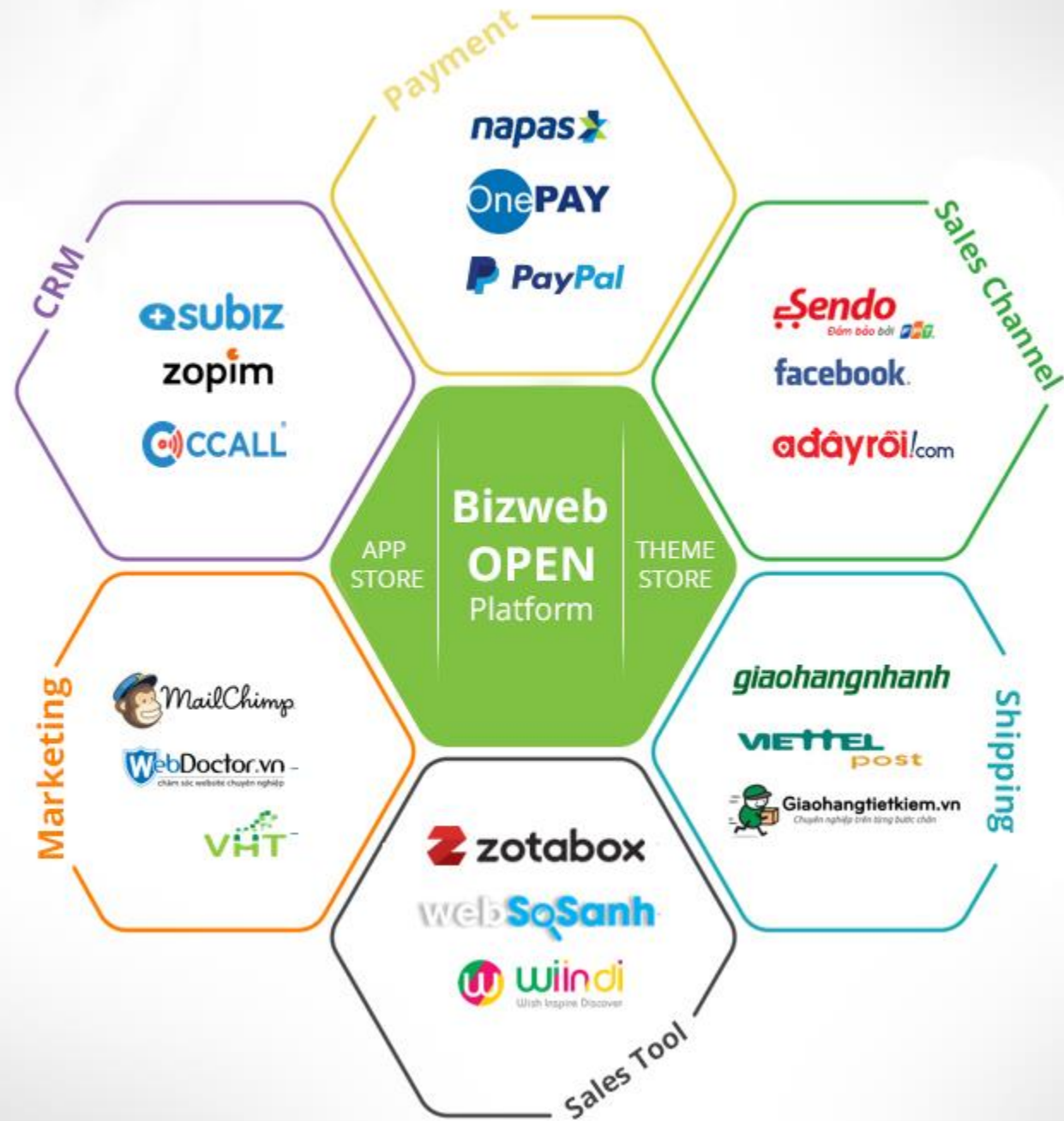


Secure REST API on Microservices

Nguyễn Minh Quý

Head of Technology at Bizweb

Bizweb.vn



Bizweb Rest API Security



Web Apps



Mobile Apps



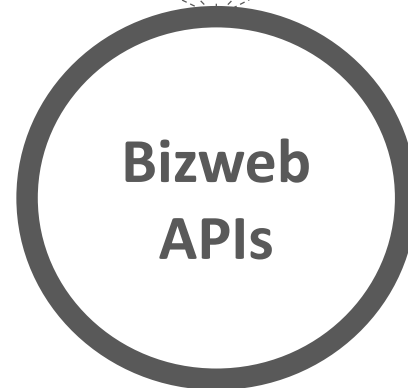
Private Apps



Public Apps



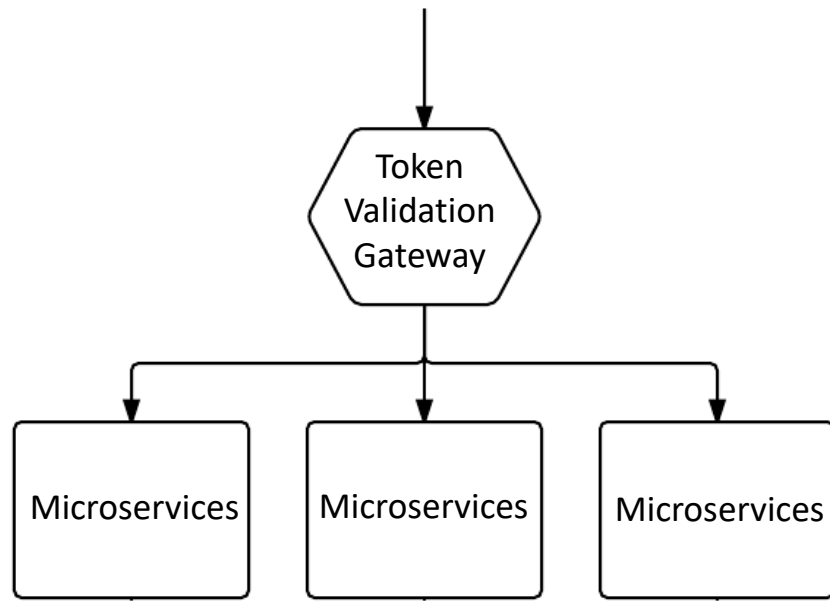
ERP Systems



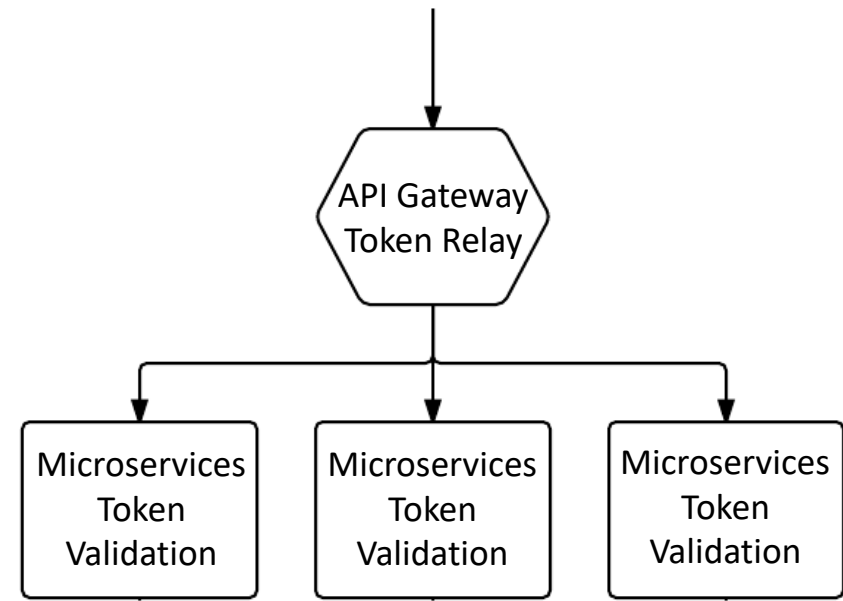
**Bizweb
APIs**

Authentication and Authorization for Microservices

1. Centralized authn/author

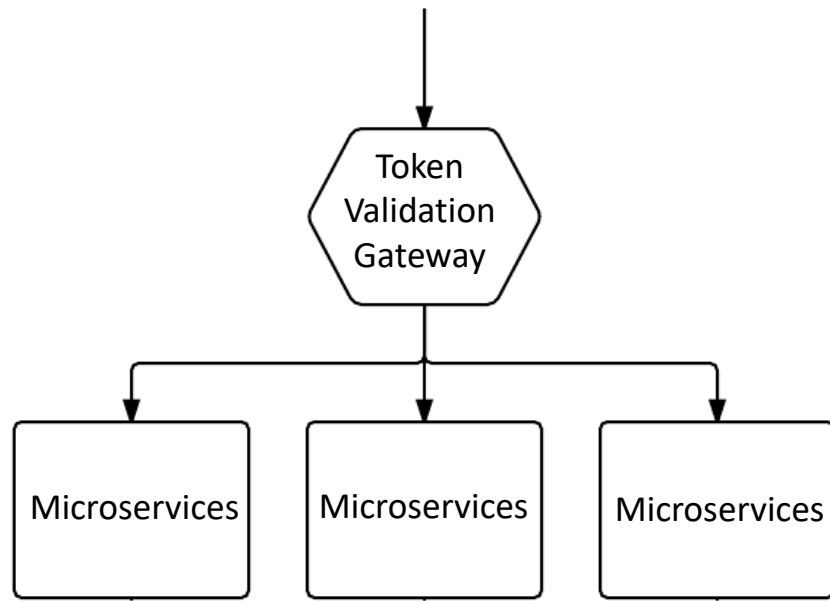


2. authn/author on each microservices

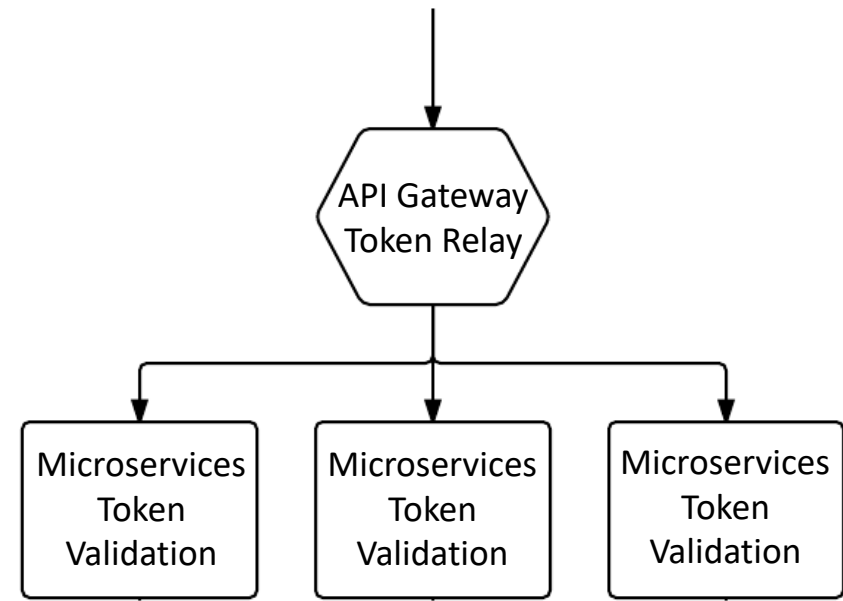


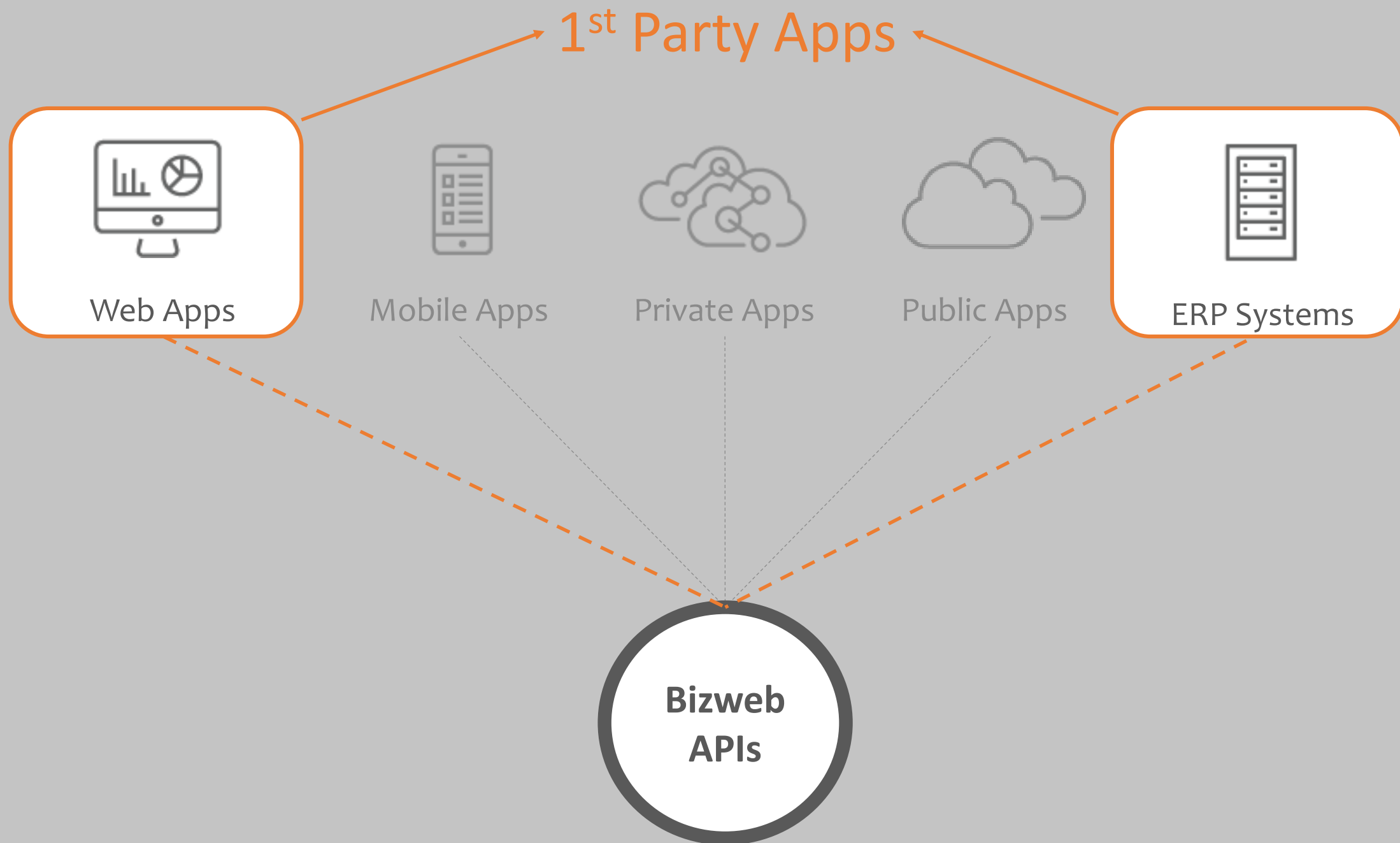
Authentication and Authorization for Microservices

1. Centralized authn/author



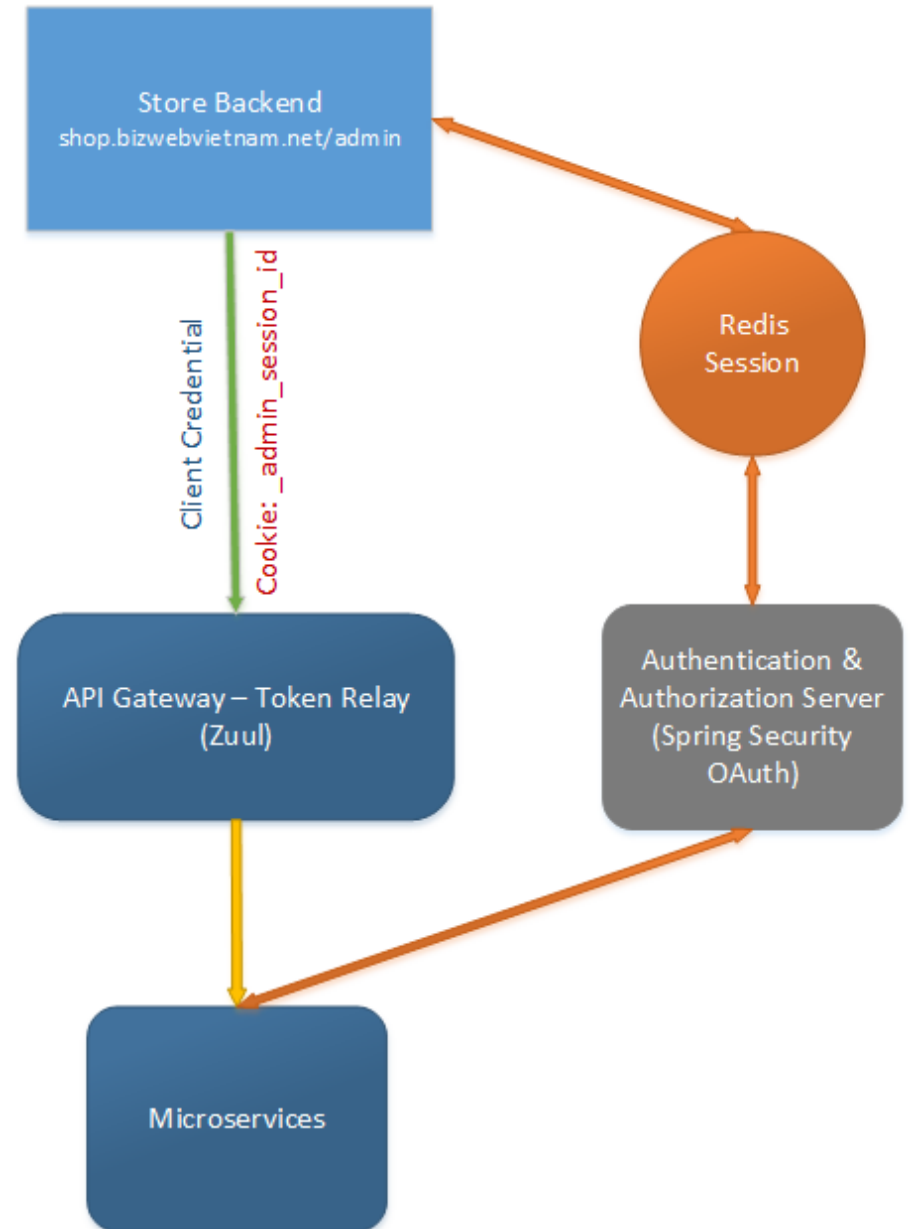
2. authn/author on each microservices





Client Credentials

- **Basic Auth + Session Auth**
- Call between microservices
- 1st App: backend, frontend, theme store, app store ...





Web Apps



Mobile Apps



Private Apps



Public Apps



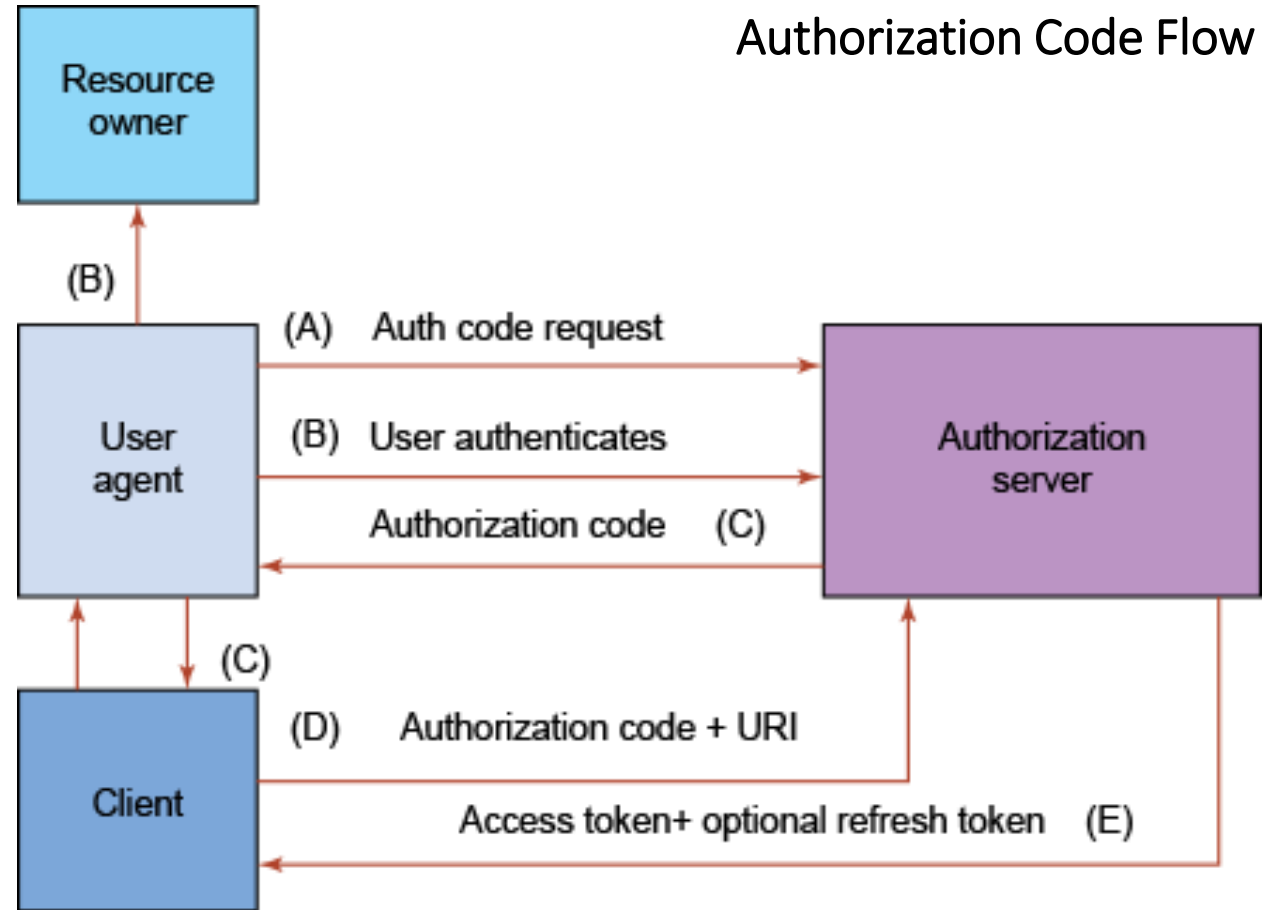
ERP Systems



Public Apps – 3rd Apps

- **OAuth 2**

- **Resource Owner (RO):** the user
- **Client:** the web or mobile app
- **Authorization Service (AS):** OAuth 2.0 server
- **Resource Server (RS):** where the actual service is stored





Web Apps



Mobile Apps



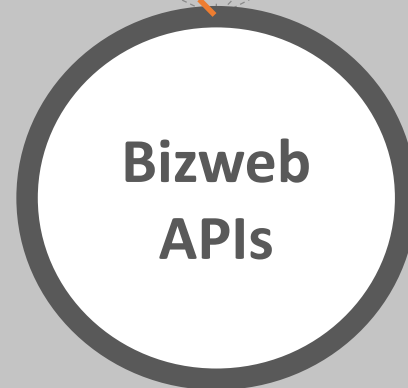
Private Apps



Public Apps



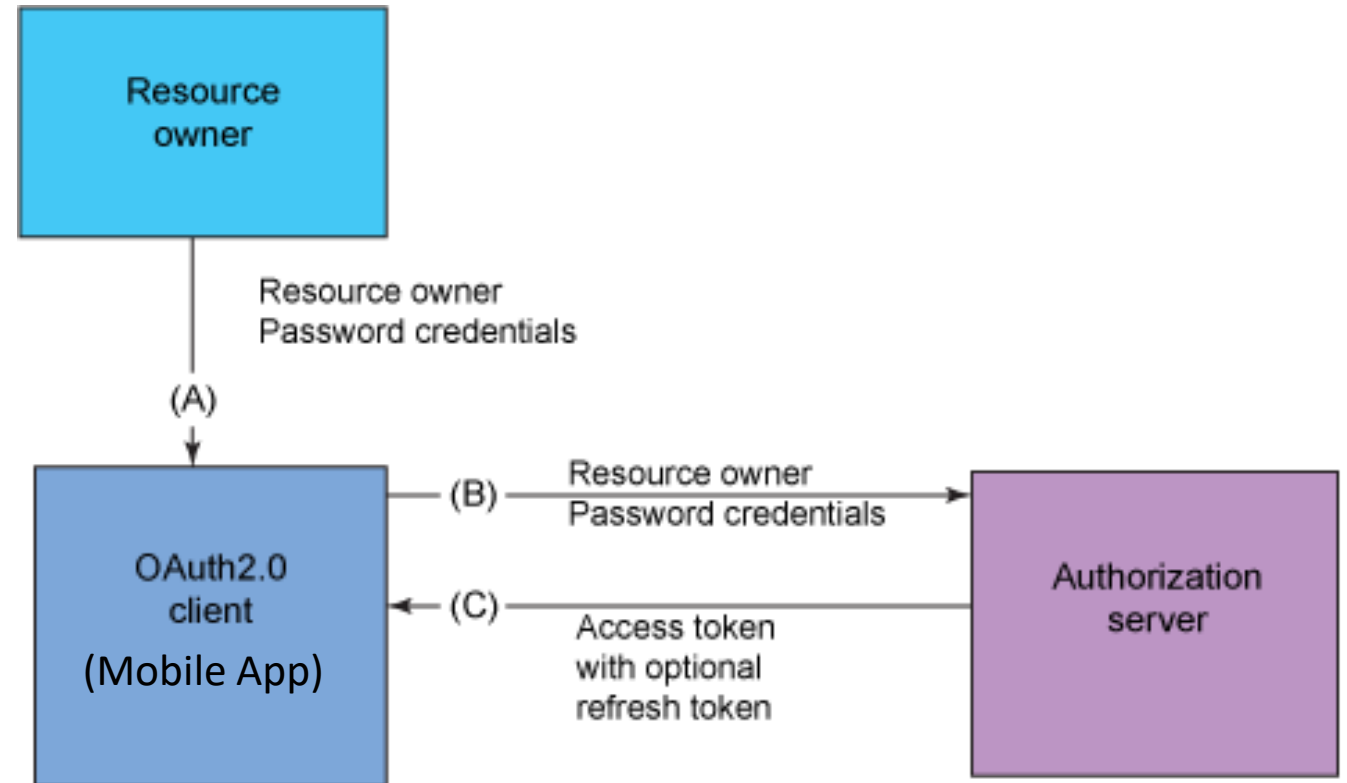
ERP Systems



**Bizweb
APIs**

xAuth - Mobile

- OAuth2
- Resource Owner Password Credentials Grant





Web Apps



Mobile Apps



Private Apps



Public Apps



ERP Systems










**Bizweb
APIs**

Basic Auth - Private Apps

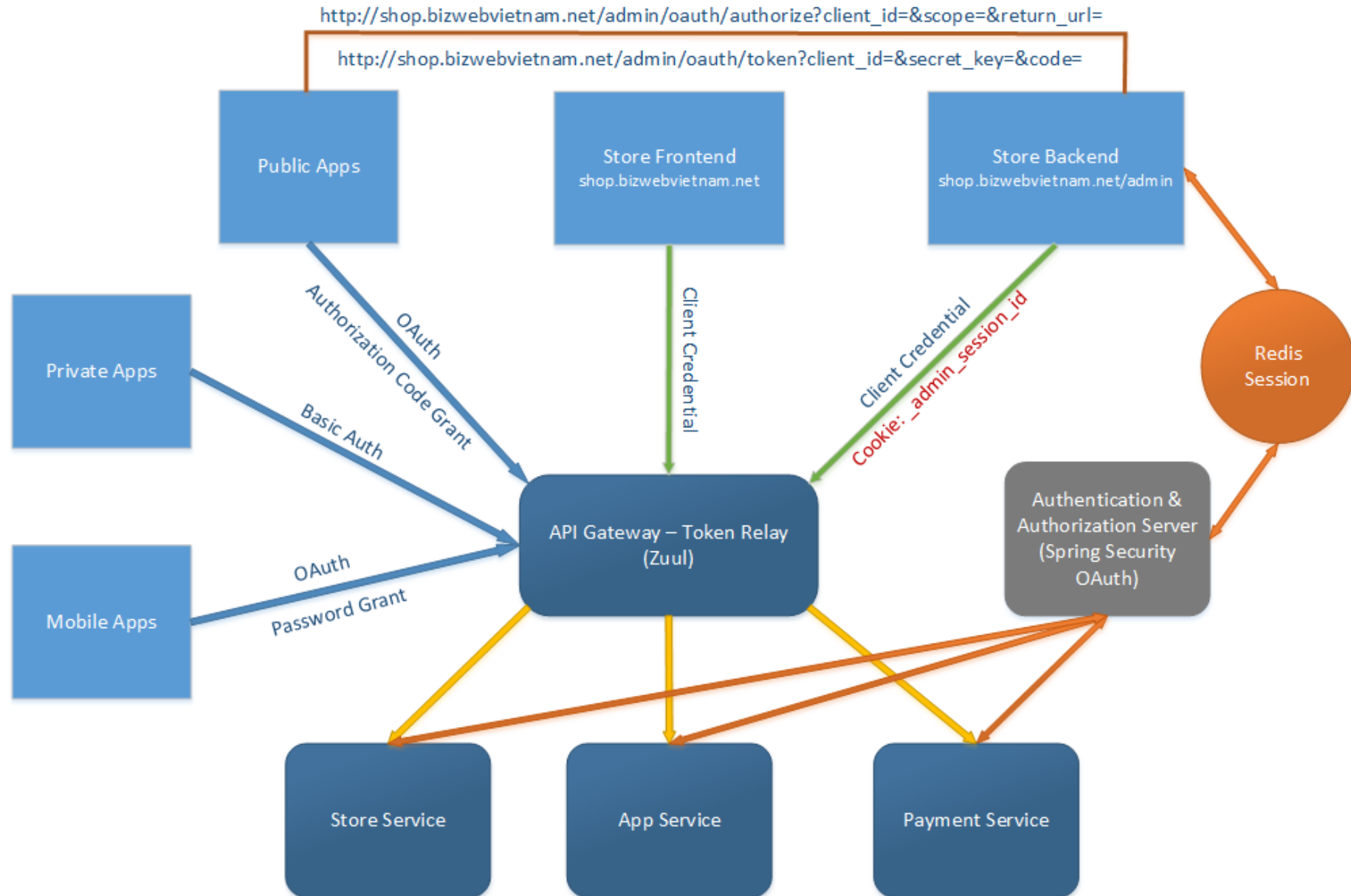
- HTTP Authentication
- HTTPS

 Private apps

Tạo Private app

Tên	API key	Secret key	Email	
Coupon	2456e5d44e23410a9ebf119d5b3c2382	4417b89ec05f483e8839cb5264ac93c0	minhquy3101@gmail.com	
Inventory	85306836be57470a938c11e3440d8379	5ac91dfc3c3548b886ca2d16c0efb552	minhquy3101@gmail.com	
Shipper	092089c3266c470889d6687d54b6b060	356d34f1c0364e29bbca8d5fa8bedb37	minhquy3101@gmail.com	
Bán hàng	f8c68b05124f429fa104790aac43e274	afc6555140514f70abe1be42d8232003	minhquy3101@gmail.com	
Partner 1	586b6789f7644cd28545821c1a1fba9f	58e0e1d96aac454fa5a0527dfdecec06	minhquy3101@gmail.com	
App bán hàng	45c7b19f8054402aac481c0857d9ec26	d7e331c78a1642ba9eeb01a9d674b170	minhquy3101@gmail.com	
App 1	96349712d9554162a262701a1cb886d1	b615f1980b4747c4a5bcb789d90b5416	minhquy3101@gmail.com	

Bizweb Authentication & Authorization



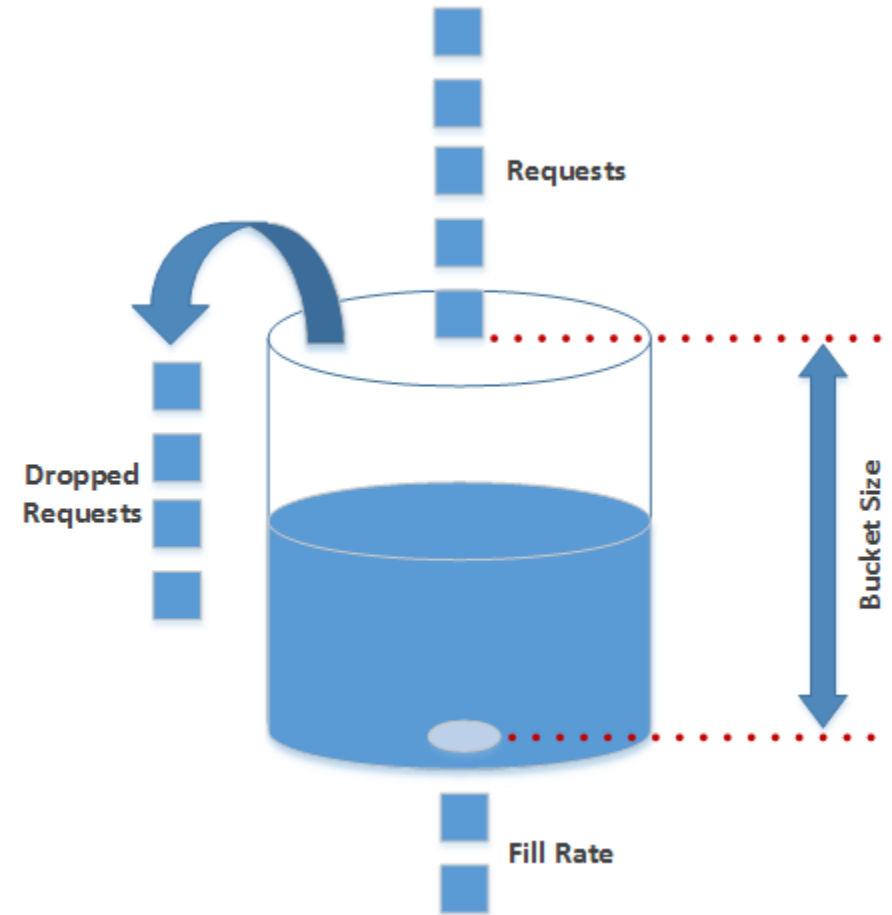
Rest API Rate Limit

Rate-Limiting Best Practices

- Authenticated
 - Have a standard, application wide rate limit
 - Custom limit for each user, application
- Unauthenticated
 - Based on domain or IP address
 - Allow limit to be overridden as well

Public API Rate Limit Filter

- Leaky Bucket algorithm (Fill Rate: 2 request/s, Bucket Size: 40)
- Http Header Response:
X-Bizweb-API-Call-Limit: 16/40
 - 16: Used requests
 - 40: Maximum requests
- When an client **exceeds** : response code 429 - Too Many Requests



API Monitoring

Why Monitor?



Why Monitor?


- You need to know if your application is working correctly
- Understand what needs to be fixed when something goes wrong
- Detect and prevent attacks

API monitoring – Key metrics


- Availability
- Throughput
- Response time
- Errors
- Notifications

API monitoring


































































Bizweb API

 Announcements

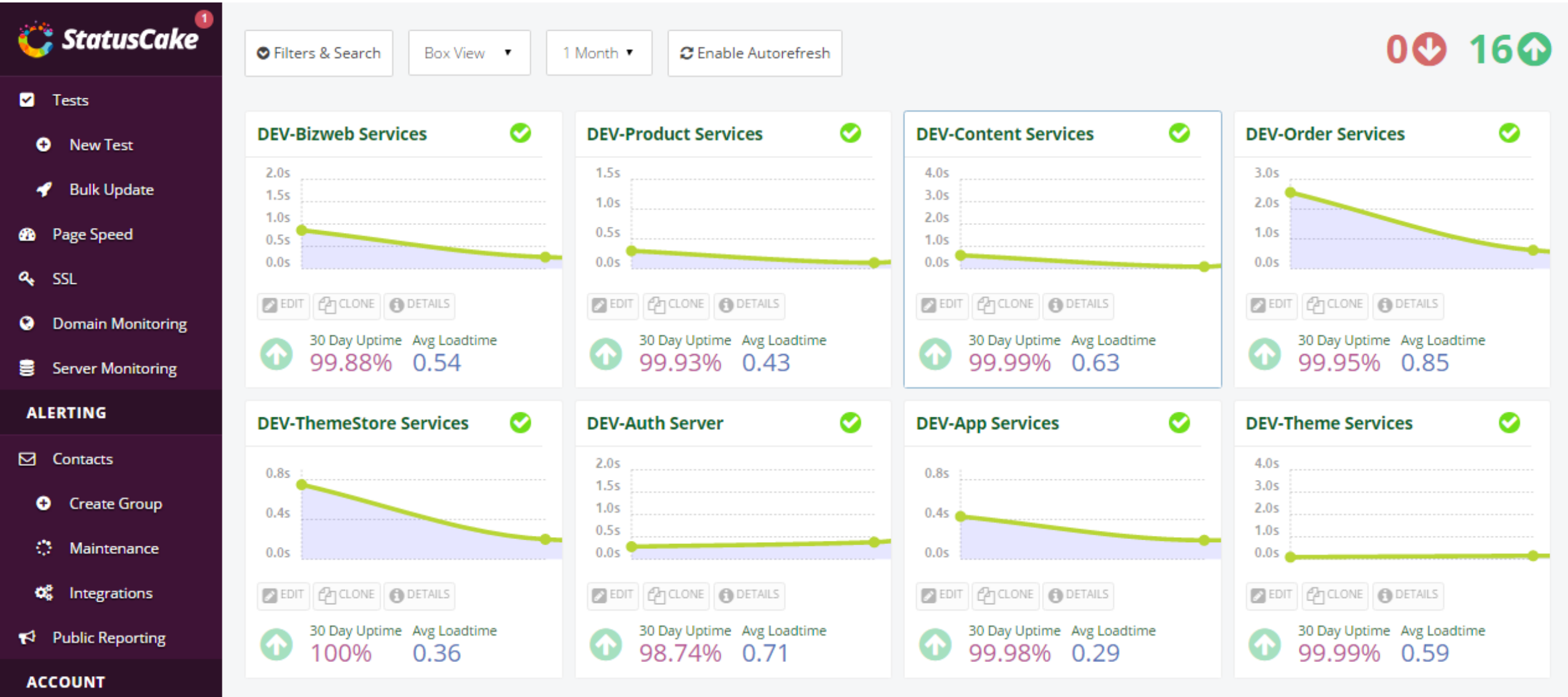
No current announcements

 7 Day Uptime

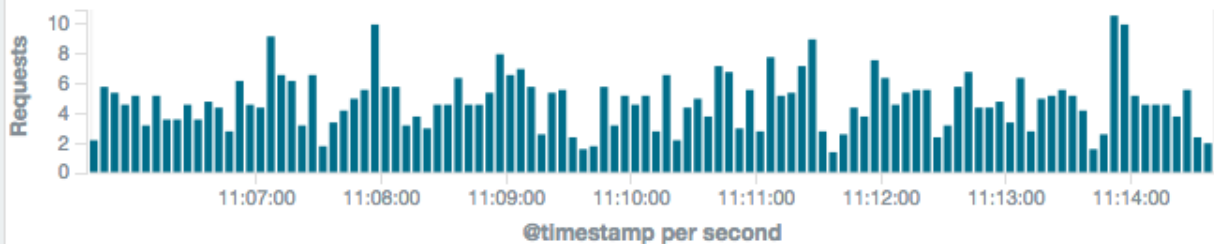
99.99%

 Uptime History									
Status	Name	Rate	Oct 13	Oct 14	Oct 15	Oct 16	Oct 17	Oct 18	Oct 19
	DEV-Order Services	1m							
	DEV-Bizweb Services	1m							
	DEV-ThemeStore Services	1m							
	DEV-Product Services	1m							
	DEV-Theme Services	1m							
	DEV-Content Services	1m							
	DEV-Auth Server	1m							
	DEV-App Services	1m							

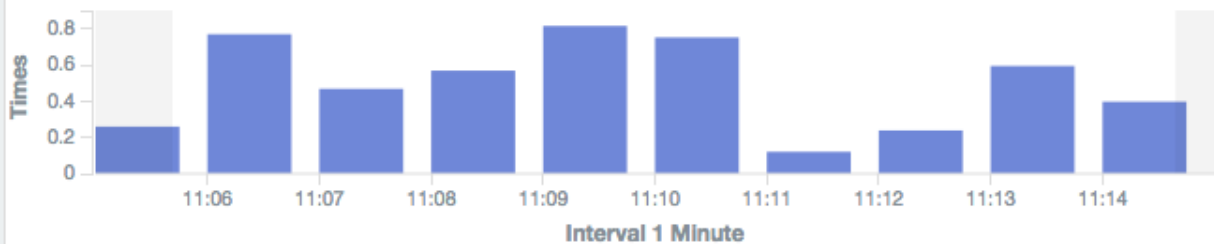
API monitoring



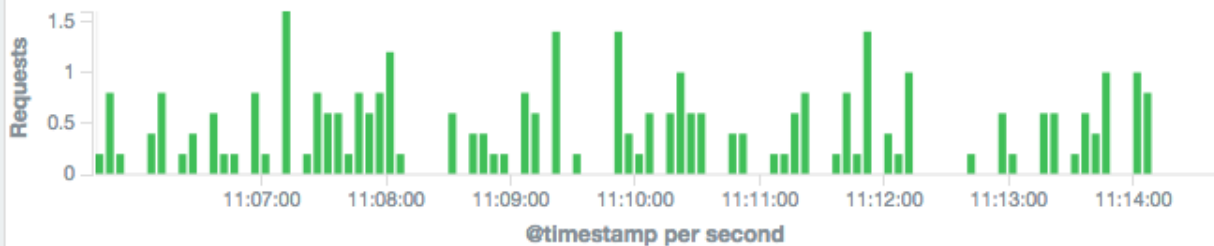
Staging - Requests



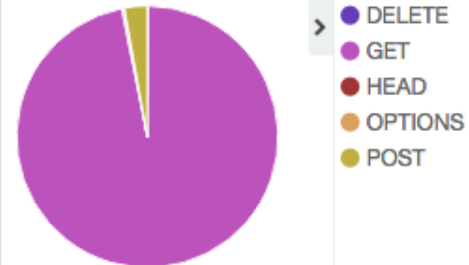
Staging - Product Average Response Time



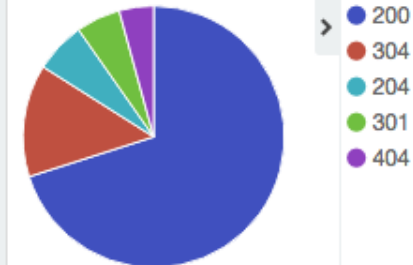
Count Admin



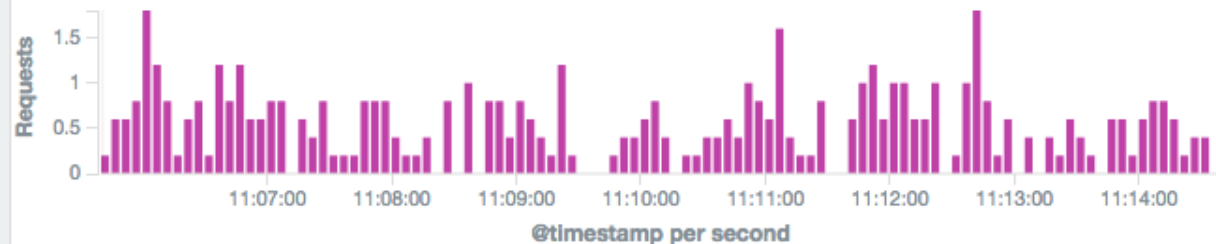
nginx-method



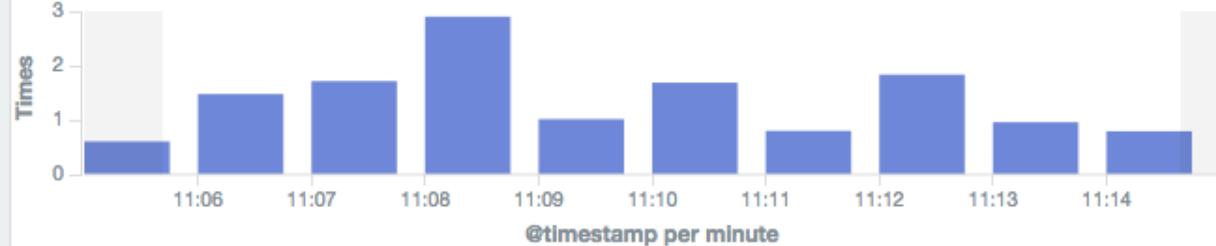
response-code



Staging - Content Requests



Staging - Content Average Response Time



Summary

- Using flexible authorization grant for microservices
- OAuth 2.0 is a standard, and has a lot of useful features
- API Rate limit
- All request to your API must be through HTTPS, reject otherwise.
- Log all request to your API

Thank you!
Q&A

