API & Identity Management Landscape

Yossi Koren – Sr. Solution Architect, API Management
Vinay Bhalerao – Sr. Solution Engineer, API Management

Oct. 31, 2017

API Security & IDP Integration

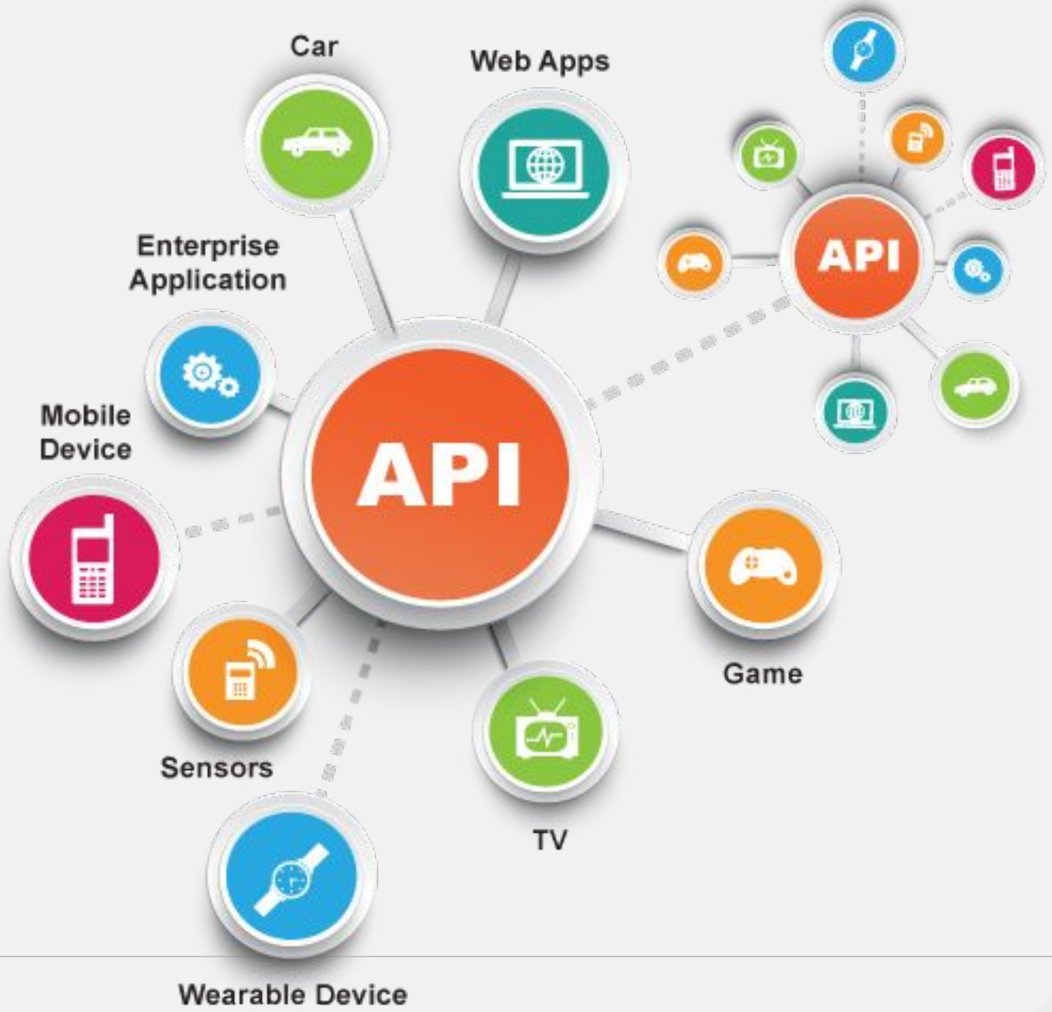
The API Security Journey

OpenID Connect (OIDC) Integration - Overview & Demo

The API Management Use-Case

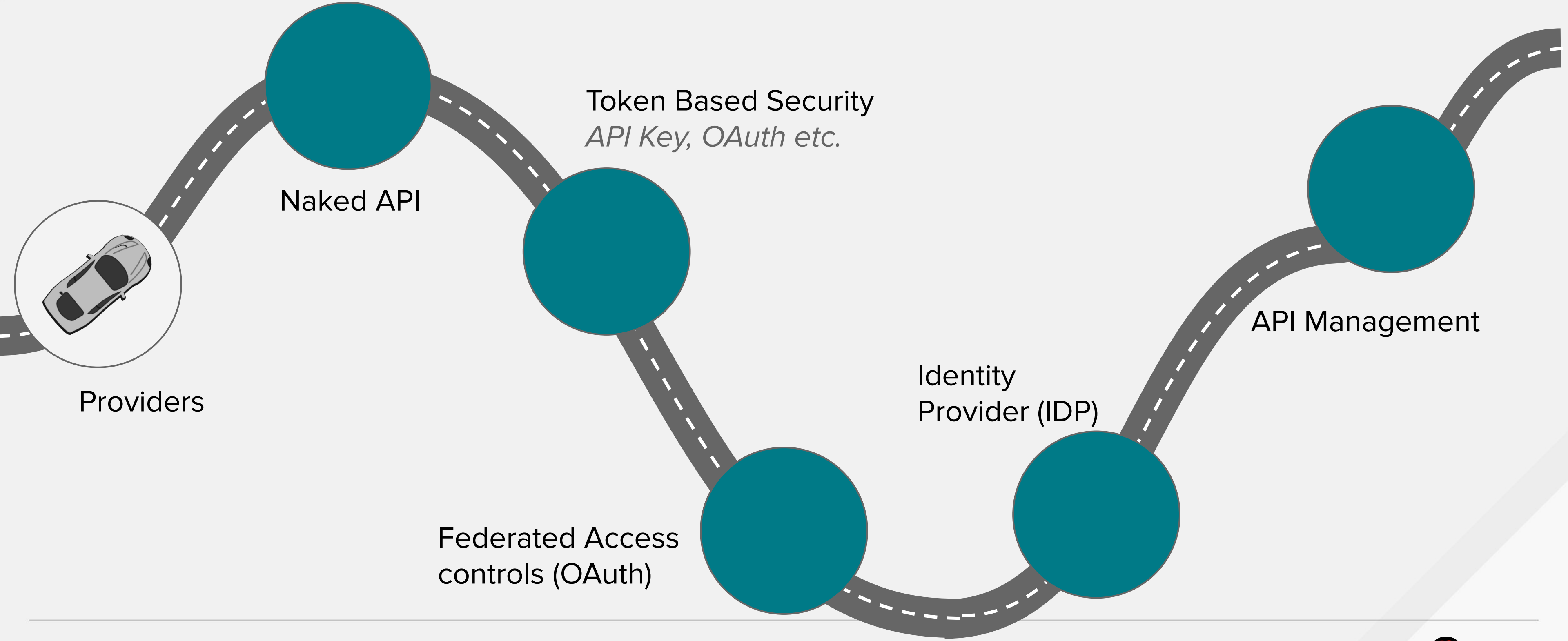
Q&A

APIs Are Everywhere!

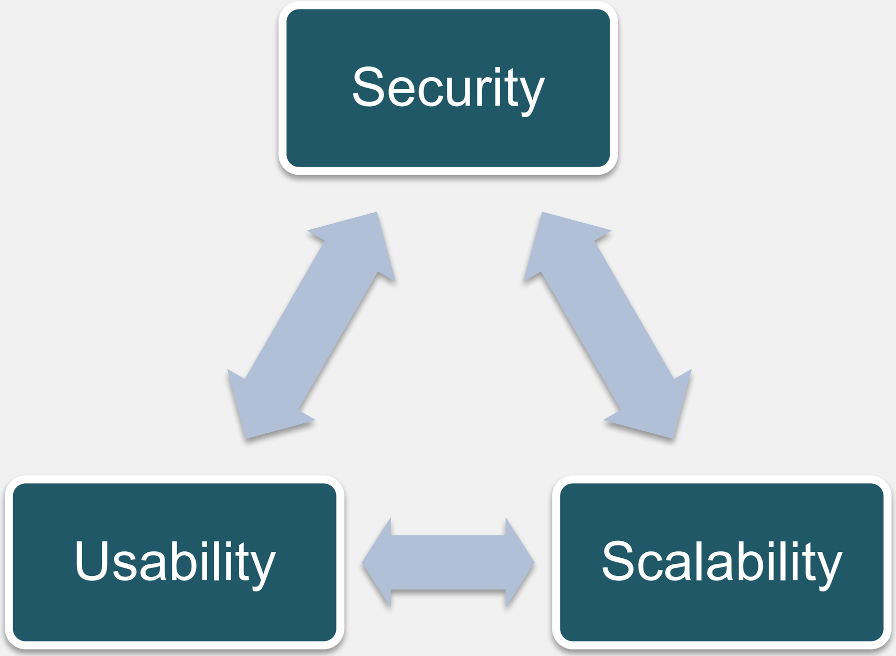


api

API Security Journey



Security, Usability and Scalability Tradeoffs



Security

Usability

Scalability

Top API Authentication Schemes

Most API Management platforms supports the following security schemes:

- **API Key** single token string
- **APP ID/APP Key (Basic Auth)** two token strings i.e. username, password
- **OAuth** authentication framework to delegate access
- **OpenID Connect (OIDC)** simple identity layer on top of OAuth framework

Identity authentication schemes

A bit more advanced but exploding in popularity is to federate access - this is enabled by OAuth

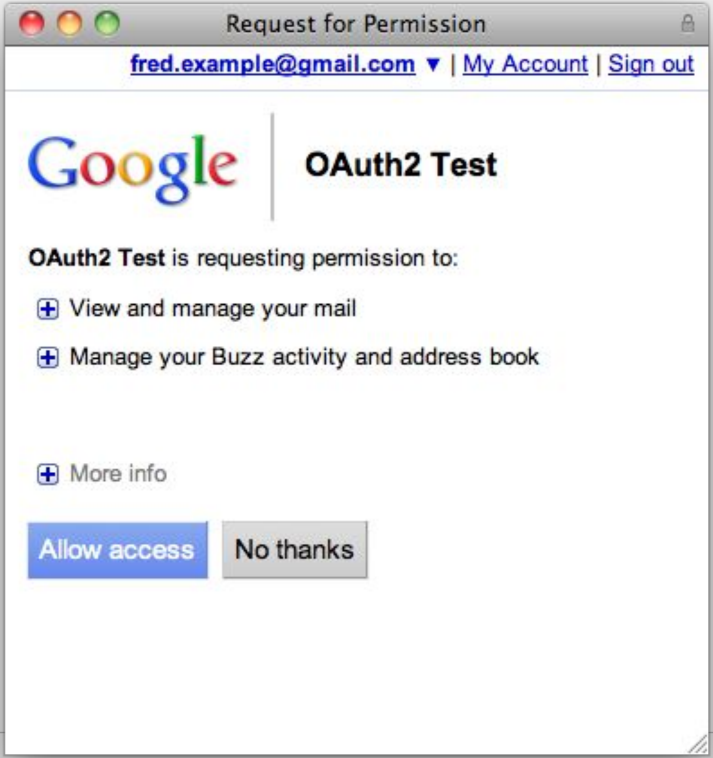
Authorization Code Flow
The most secure and used where a user logs into Identity server and grants access to Application to retrieve their data

Client Credentials Flow
Only Application data is passed in a single request for an Access Token

Implicit Flow
User logs in but secret is not passed

Resource Owner Password Flow
Application, username and password data is passed in a single request for an Access Token

OAuth enables people delegate access to apps to act on our behalf



Request for Permission

fred.example@gmail.com ▼ | My Account | Sign out

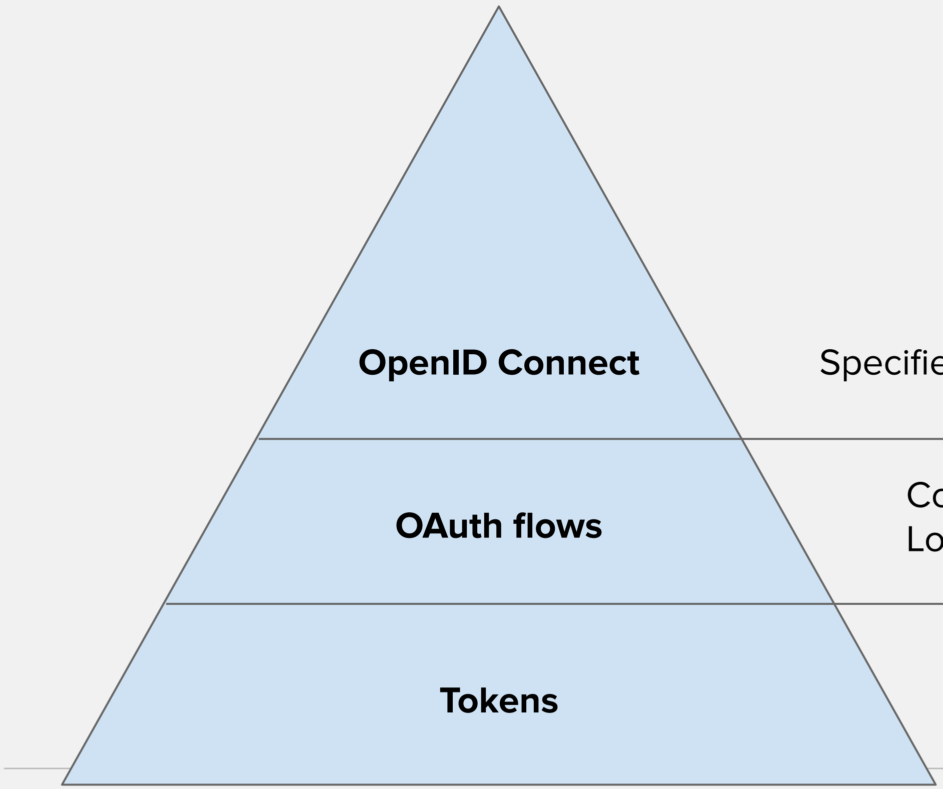
OAuth2 Test

OAuth2 Test is requesting permission to:

- View and manage your mail
- Manage your Buzz activity and address book

More info

Layered Security Standards



OpenID Connect

Specifies JWT for token, and some extensions

OAuth flows

Core delegation flows.
Lots (too much?) flexibility

Tokens

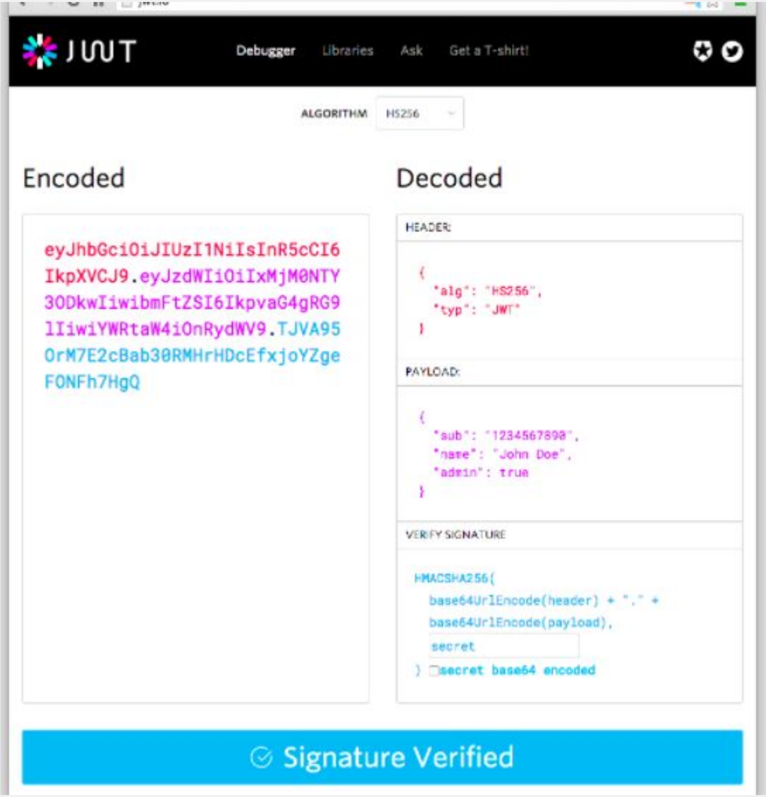
Wide variety of token and encryption standards

OpenID
Connect

OpenID Connect (OIDC)

- OpenID Connect : built on top of the OAuth 2.0 protocol
- Allows clients to verify the identity of an end user
- Obtains basic profile information about the end user
- RESTful HTTP API, using JSON as a data format

JWT ("jot") Example



ALGORITHM HS256

Encoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6
IkpXVCJ9.eyJzdWIiOiIxMjM0NTY
3ODkwIiwibmFtZSI6IkpvaG4gRG9
lIiwiYWRtaW4iOnRydWV9.TJVA95
OrM7E2cBab30RMHrHDcEfxjoYZge
FONFh7HgQ
```

Decoded

HEADER:

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD:

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

VERIFY SIGNATURE

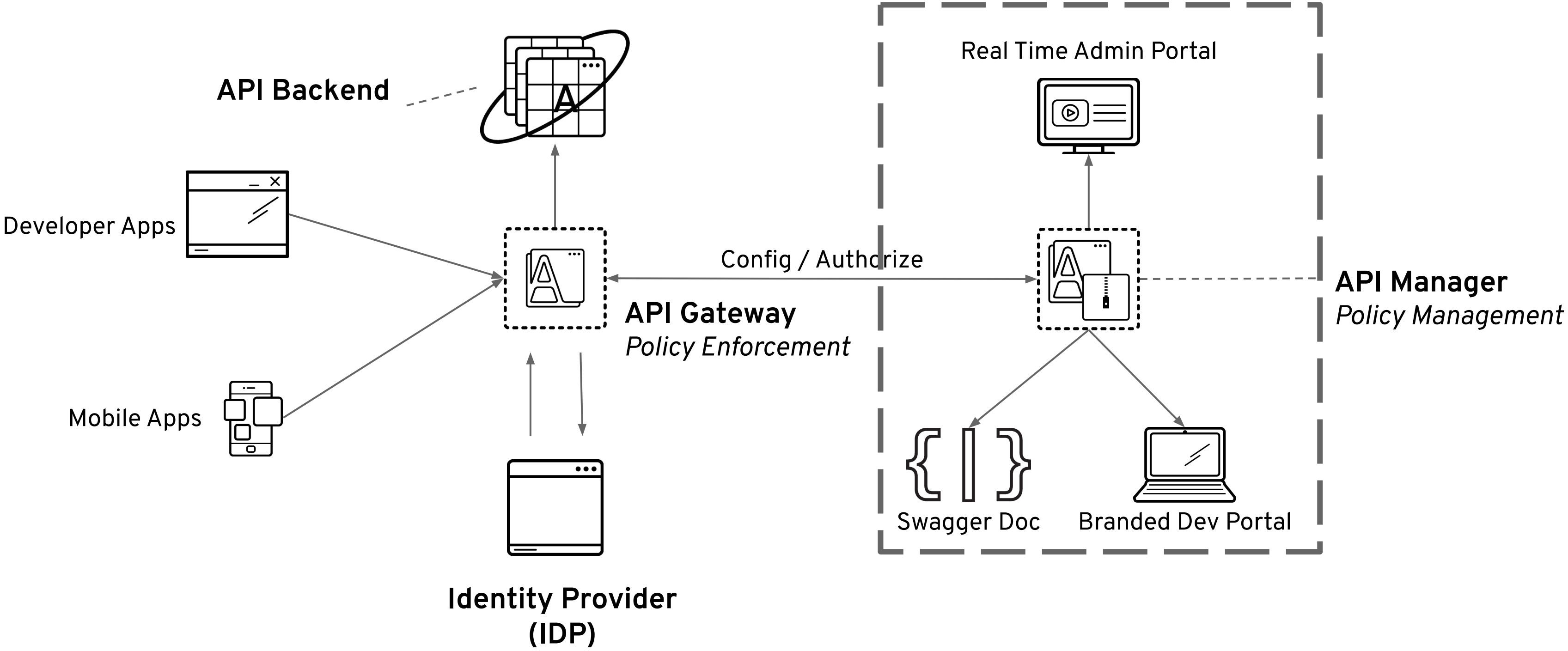
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
) □secret base64 encoded
```

Signature Verified

JWT (“jot”) to the rescue

- Signed by algo and verified by only correct key
- Contains user identity in form of claims (Private, public, reserved)
- For OIDC purpose, SSO is widely adopted in consumer/enterprise apps
- Eliminates the need to look up against a central access control list

System Architecture

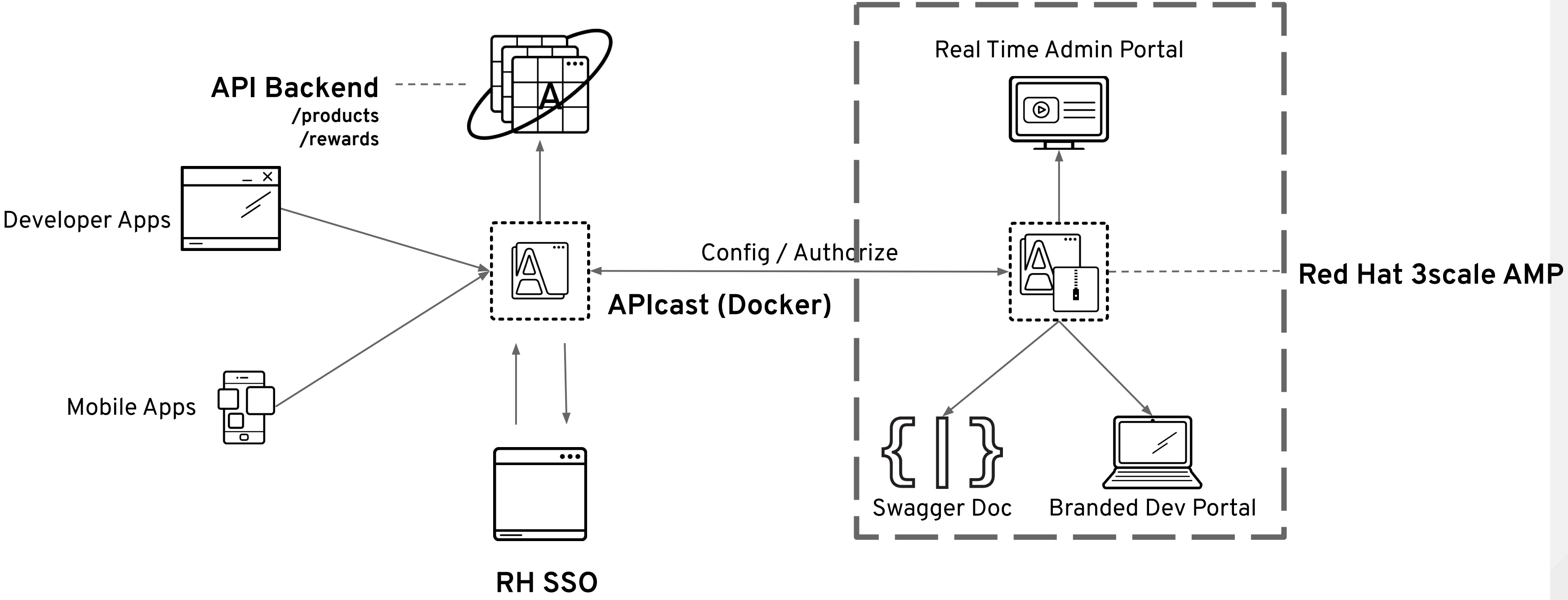


System Architecture

The 3scale API Management architecture consists of :

- The **API Manager** which manages the API, Developers and Applications
- The **Traffic Manager** (API Gateways) that enforce the policies from the API Manager and delegate authorization to 3rd party IDPs
- The **Identity Provider (IDP)** identity hub that supports many authentication using various protocols
- The **API Backend** the API. i.e. the API Provider

Demo Overview



Demo Overview

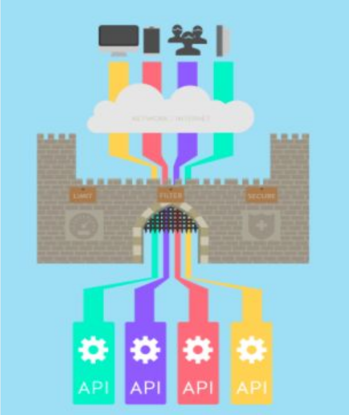
- API Manager - Red Hat 3scale AMP
- API backend - https://echo-api.3scale.net:443
- API Endpoints
    - Rewards
    - Products
- App Security - OIDC Authorization code Workflow
- IDP - RH-SSO
- API Gateway - APIcast (Docker)

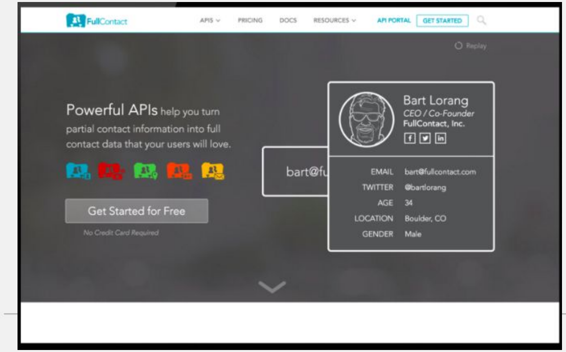
Deployment Steps

- Setting up API Manager - Setup the private API, Application and Security scheme
    - Enable sign-up workflow
    - Generate Client Id, Client Secret and sync credentials with IDP
- Setting up IDP (RH-SSO)
    - Client details
    - Grant Type
- Deploy API Gateway (Docker image)
- Invoke API Request from client application

API Provider Challenges….

API Management Added Value





Powerful APIs help you turn partial contact information into full contact data that your users will love.

No Credit Card Required

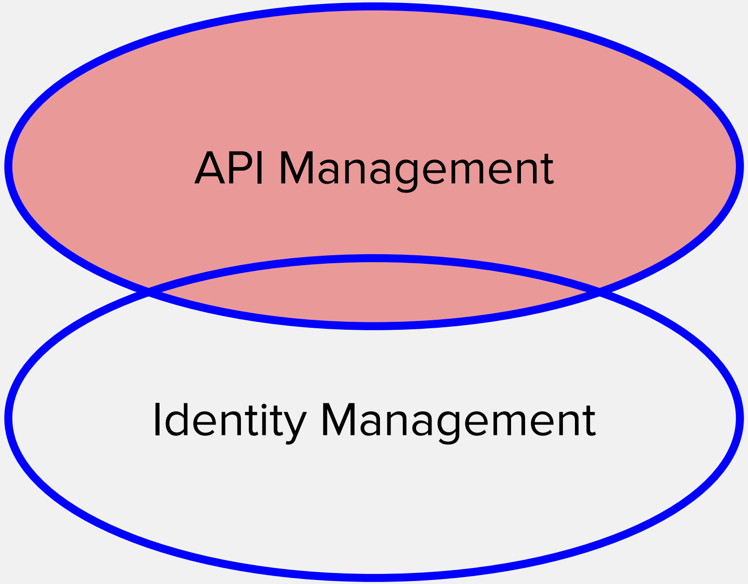
bart@fu

Bart Lorang
CEO / Co-Founder
FullContact, Inc.

EMAIL	bart@fullcontact.com
TWITTER	@bartlorang
AGE	34
LOCATION	Boulder, CO
GENDER	Male

APIs

Converged Access Management



Red Hat 3scale Online Resources

Red Hat Training Portal
https://www.redhat.com/en/services/training/all-courses-exams

Red Hat 3scale API Management
https://www.redhat.com/en/technologies/jboss-middleware/3scale

Red Hat 3scale API Management - Hands-On Workshop
https://www.redhat.com/en/events/hands-on-api-management-3scale

Thank You!