Modern Identity Management

in the era of Serverless and Microservices

VERSION 1.4

EQUIFAX

Had Been Uploaded

38,000
Driver's Licenses

3,200
Passport Details

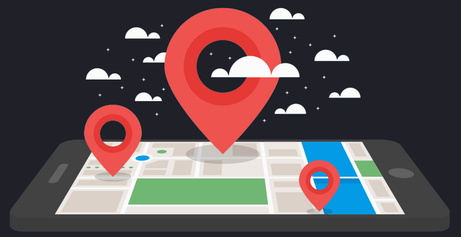
@itrjwyss

Oracle
Groundbreaker
Ambassador

Had Stolen

146.6 million
Names and Dates
of Birth

145.5 million
Social Security
Numbers



99 million
Address

209,000 Payment
Card Numbers and
Expiration Dates

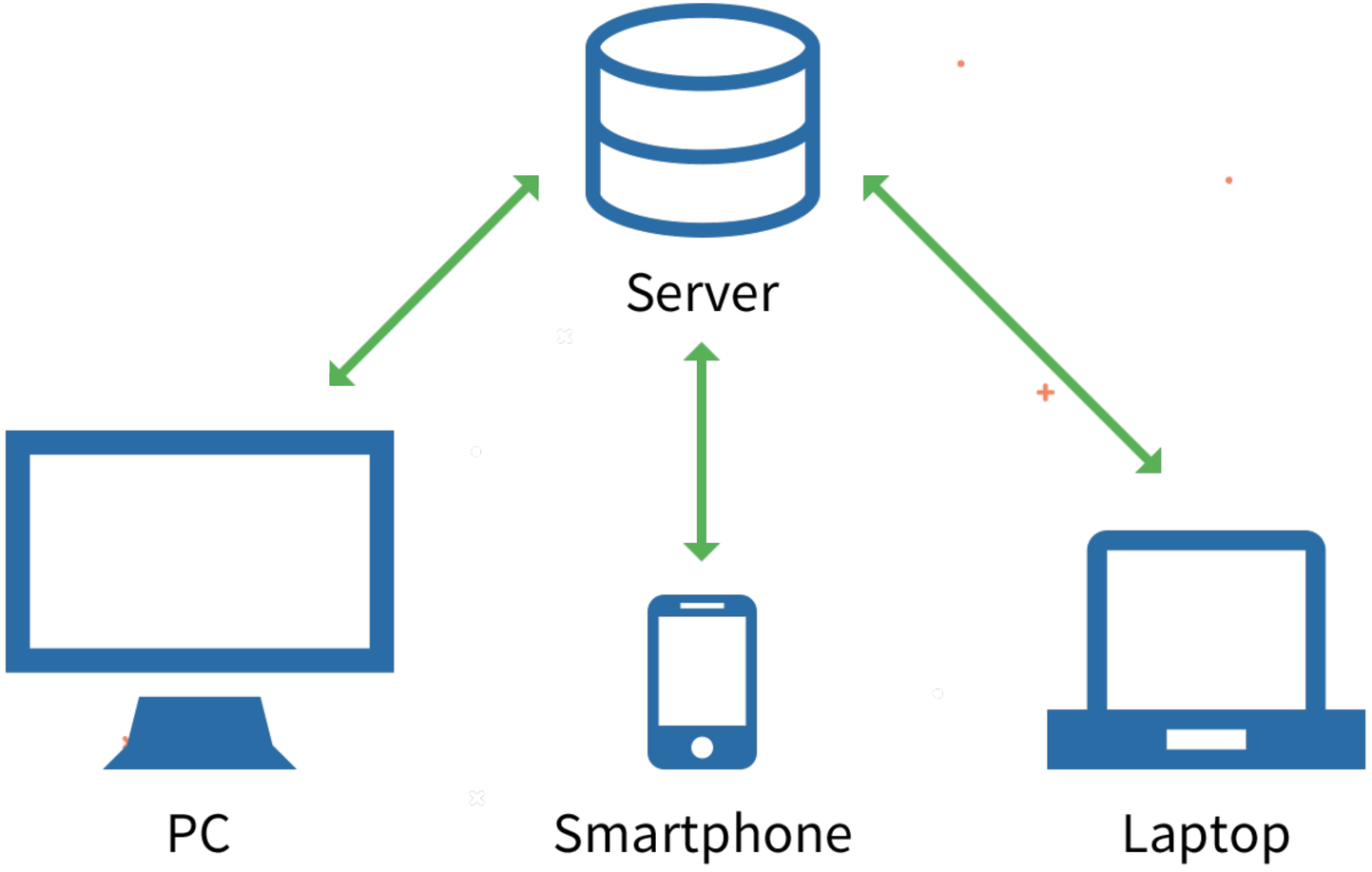
@itrjwyss

EU General Data Protection Regulation

25 May 2018

Oracle Groundbreaker Ambassador

Security is a **Team Effort**



@itrjwyss

Agenda

- Rest API Design / OAuth
- JWT
- User Credentials Problem
- Identity Management (IdM)
- Identity and Access Management (IAM)
- How to have a successful Identity Management Project
- IdM in Serverless and Microservices Architectures
- Identity as a Service (IDaaS)

Mercedes Wyss

@itrjwyss

Community Leader

Devs+502 & JDuchess Chapter Guatemala

Ex-JUG Member

Guatemala Java Users Group (GuateJUG)

Chief Technology Officer (CTO) at Produactivity

Full Stack Developer

Auth0 Ambassador &
Oracle Groundbreaker Ambassador

Duke's Choice Award
2016 Winner
Java

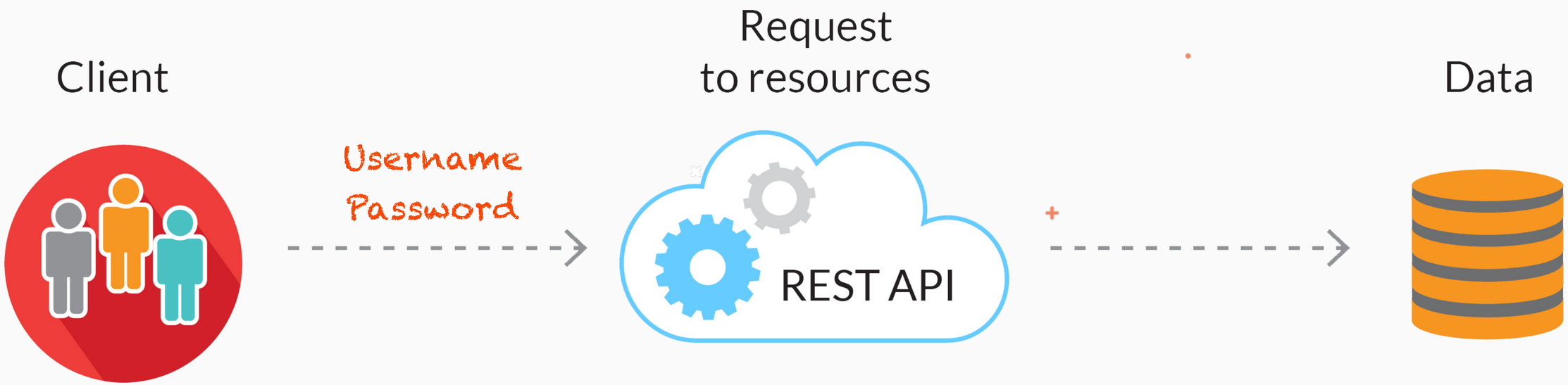
AMBASSADOR

Oracle Groundbreaker Ambassador

Devs +502
Comunidad Desarrolladores en Tecnologías
< Google > en Guatemala

JDuchess Guatemala

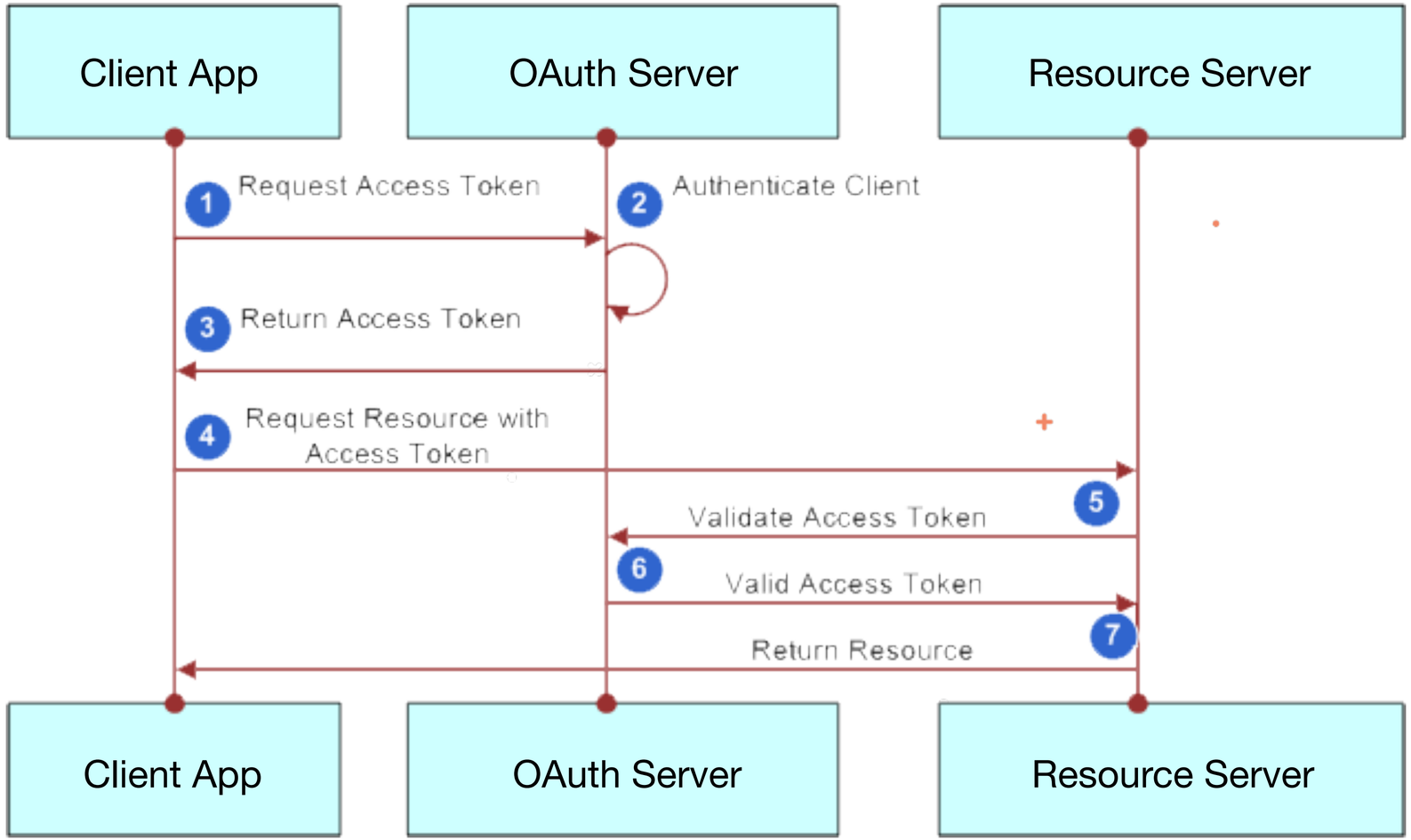
Bad API Design



@itrjwyss

Oracle
Groundbreaker
Ambassador

OAuth



@itrjwyss

JWT

@itrjwyss

Oracle
Groundbreaker
Ambassador

Is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

@itrjwyss

AMBASSADOR

Header

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.

Claims

JSON Web Signature
JWT + JWS

@itrjwyss

AMBASSADOR

Signature Algorithms

JWS	Algorithm	Description
HS256	HMAC256	HMAC with SHA-256
HS384	HMAC384	HMAC with SHA-384
HS512	HMAC512	HMAC with SHA-512
RS256	RSA256	RSASSA-PKCS1-v1_5 with SHA-256
RS384	RSA384	RSASSA-PKCS1-v1_5 with SHA-384
RS512	RSA512	RSASSA-PKCS1-v1_5 with SHA-512
ES256	ECDSA256	ECDSA with curve P-256 and SHA-256
ES384	ECDSA384	ECDSA with curve P-384 and SHA-384
ES512	ECDSA512	ECDSA with curve P-521 and SHA-512

Exploring JWT


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
.
eyJqdGkiOiI1MWQ4NGFjMS1kYjMxLTRjM2ItOTQwOS1lNjMwZWJiYj
gzZGYiLCJ1c2VybmFtZSI6Imh1bnRlcjIiLCJzY29wZXMiOlsicmVw
bzpyZWFkIiwiZ2lzdDp3cml0ZSJdLCJpc3MiOiIxNDUyMzQzMzcyIi
wiZXhwIjoiMTQ1MjM0OTM3MiJ9
.
cS5KkPxtEJ9eonvsGvJBZFIamDnJA7gSz3HZBWv6S1Q
```


@itrjwyss

Exploring JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9 Header

.

eyJqdGkiOiI1MWQ4NGFjMS1kYjMxLTRjM2ItOTQwOS1lNjMwZWJiYjgzZGYiLCJ1c2VybmFtZSI6Imh1bnRlcjIiLCJzY29wZXMiOlsicmVwbzpyZWFkIiwiZ2lzdDp3cml0ZSJdLCJpc3MiOiIxNDUyMzQzMzcyIiwiZXhwIjoiMTQ1MjM0OTM3MiJ9

Claims

.

cS5KkPxtEJ9eonvsGvJBZFIamDnJA7gSz3HZBWv6S1Q Signature

@itrjwyss

AMBASSADOR

Exploring JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "jti": "51d84ac1-db31-4c3b-9409-e630ebbb83df",
  “sub": "hunter2",
  "scopes": ["repo:read", "gist:write"],
  "iss": "1452343372",
  "exp": "1452349372"
}
.
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

@itrjwyss

Oracle Groundbreaker Ambassador

Exploring JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "jti": "51d84ac1-db31-4c3b-9409-e630ebbb83df",
  “sub": "hunter2",
  "scopes": ["repo:read", "gist:write"],
  "iss": "1452343372",
  "exp": "1452349372"
}
.
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

@itrjwyss

Oracle Groundbreaker Ambassador

Exploring JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "jti": "51d84ac1-db31-4c3b-9409-e630ebbb83df",
  “sub": "hunter2",
  "scopes": ["repo:read", "gist:write"],
  "iss": "1452343372",
  "exp": "1452349372"
}
.
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

@itrjwyss

Oracle Groundbreaker Ambassador

Exploring JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "jti": "51d84ac1-db31-4c3b-9409-e630ebbb83df",
  “sub": "hunter2",
  "scopes": ["repo:read", "gist:write"],
  "iss": "1452343372",
  "exp": "1452349372"
}
.
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

@itrjwyss

Oracle Groundbreaker Ambassador

Registered Claims

iss	The issuer of the token
sub	The subject of the token
aud	The audience of the token
exp	The expiration in NumericDate value
nbf	sbt configuration files
iat	The time the JWT was issued
jti	Unique identifier for the JWT

Registered Claims

iss	The issuer of the token
sub	The subject of the token
aud	The audience of the token
exp	The expiration in NumericDate value
nbf	sbt configuration files
iat	The time the JWT was issued
jti	Unique identifier for the JWT

Registered Claims

iss	The issuer of the token
sub	The subject of the token
aud	The audience of the token
exp	The expiration in NumericDate value
nbf	sbt configuration files
iat	The time the JWT was issued
jti	Unique identifier for the JWT

Registered Claims

iss	The issuer of the token
sub	The subject of the token
aud	The audience of the token
exp	The expiration in NumericDate value
nbf	sbt configuration files
iat	The time the JWT was issued
jti	Unique identifier for the JWT

Registered Claims

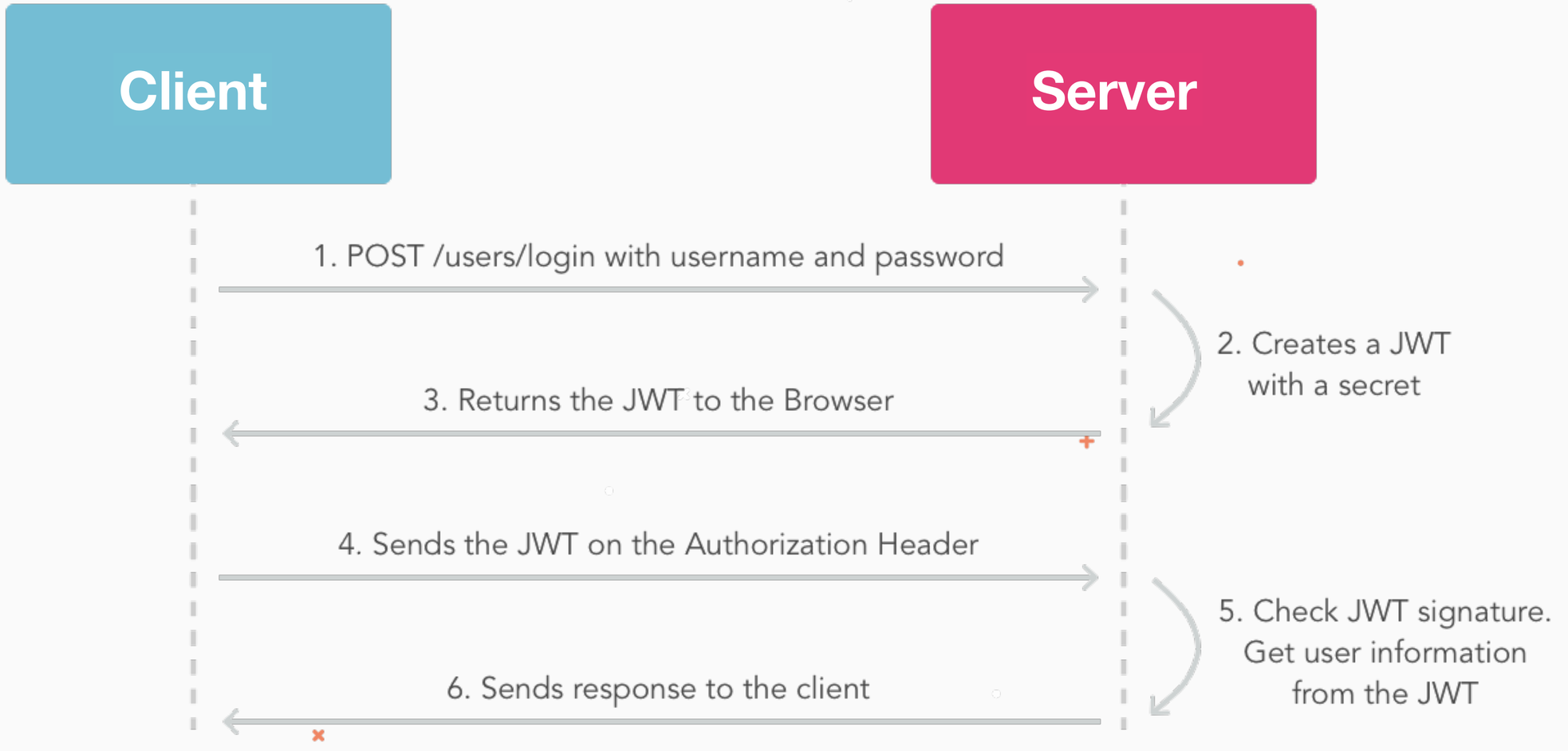
iss	The issuer of the token
sub	The subject of the token
aud	The audience of the token
exp	The expiration in NumericDate value
nbf	sbt configuration files
iat	The time the JWT was issued
jti	Unique identifier for the JWT

What problems does JWT solve?

- Authentication
- Authorization
- Federated Identity
- Information Exchange
- Client-side Sessions (“stateless” sessions)
- Client-side Secrets

What problems does JWT solve?

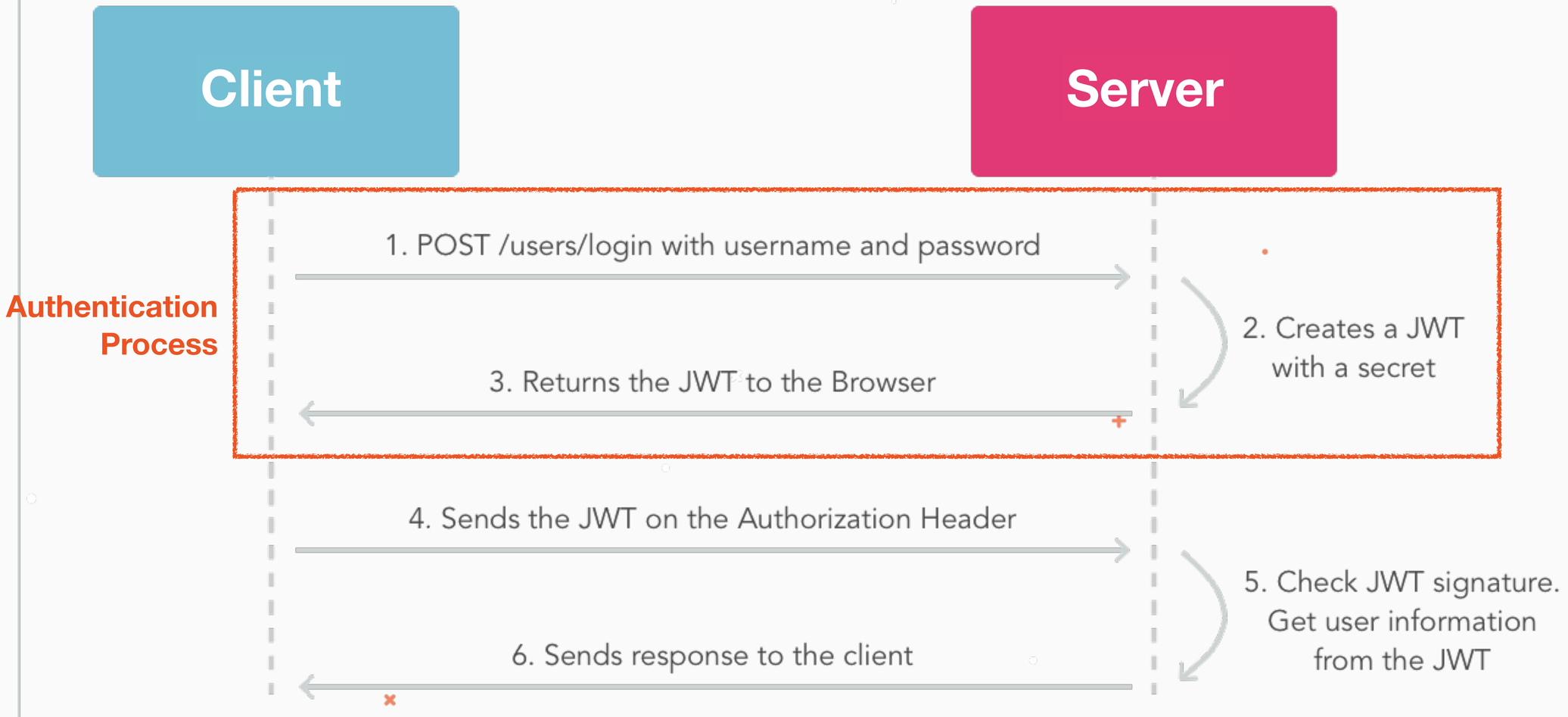
- Authentication
- Authorization
- Federated Identity
- Information Exchange
- Client-side Sessions (“stateless” sessions)
- Client-side Secrets



Auth0 (June 2017) https://cdn.auth0.com/content/jwt/jwt-diagram.png

@itrjwyss

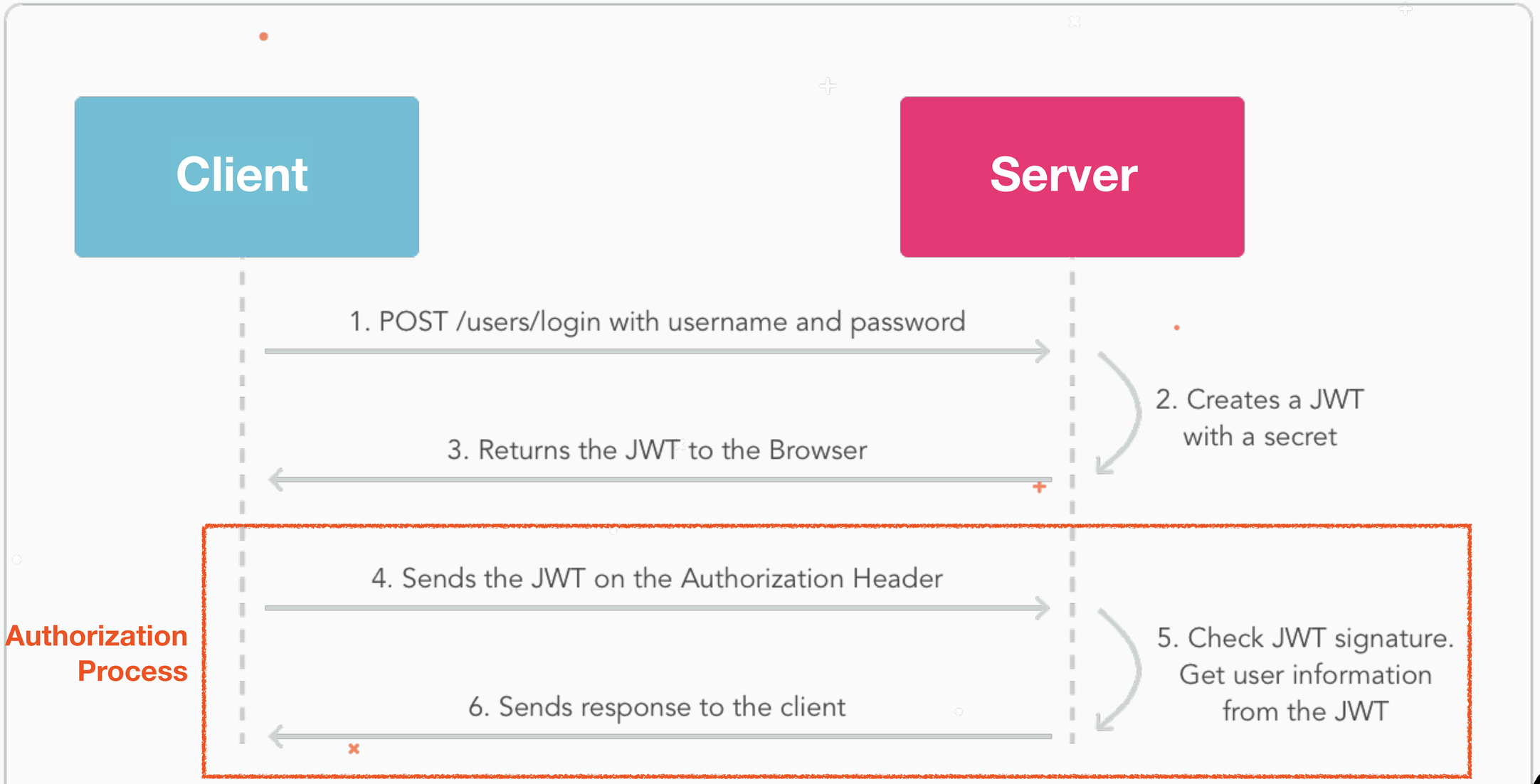
AMBASSADOR



Auth0 (June 2017) https://cdn.auth0.com/content/jwt/jwt-diagram.png

@itrjwyss

AMBASSADOR



Auth0 (June 2017) https://cdn.auth0.com/content/jwt/jwt-diagram.png

@itrjwyss

AMBASSADOR

Seguro | https://jwt.io

JWT

Debugger Libraries Introduction Ask Get a T-shirt!

Crafted by Auth0

Debugger

ALGORITHM HS256

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdW
IiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lI
iwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrH
DcEfxjoYZgeFONFh7HgQ
```


Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "sub": "1234567890",
```

Oracle Groundbreaker Ambassador

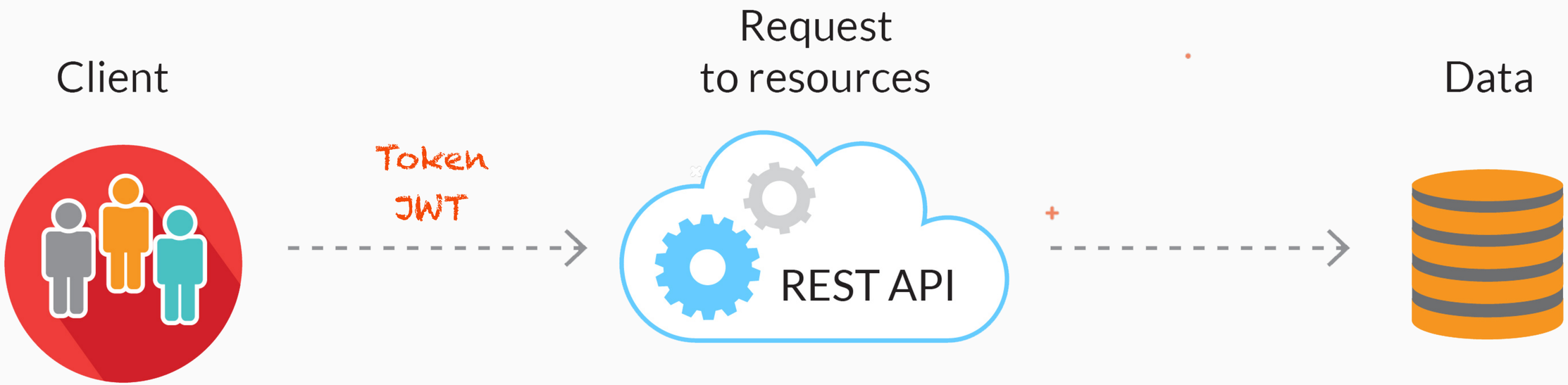
Learn everything you wanted to know, but were afraid to ask about JSON Web Tokens

auth0.com/e-books/jwt-handbook

@itrjwyss

AMBASSADOR

Improve API Design



@itrjwyss

Oracle
Groundbreaker
Ambassador

User Credentials Problem

@itrjwyss

SSO

Single Sign On

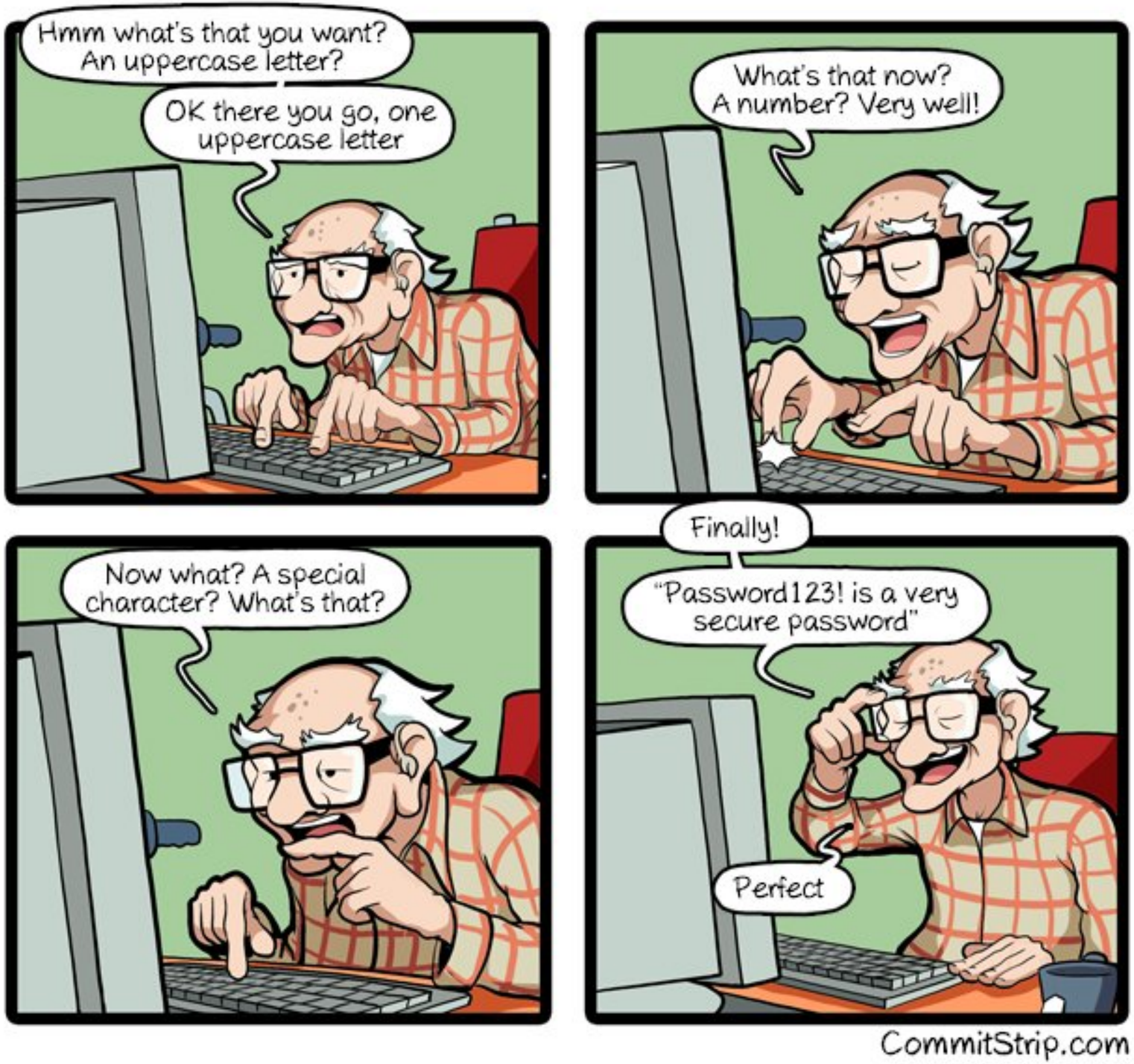
@itrjwyss

Oracle
Groundbreaker
Ambassador

PASSWORD
AMBASSADOR

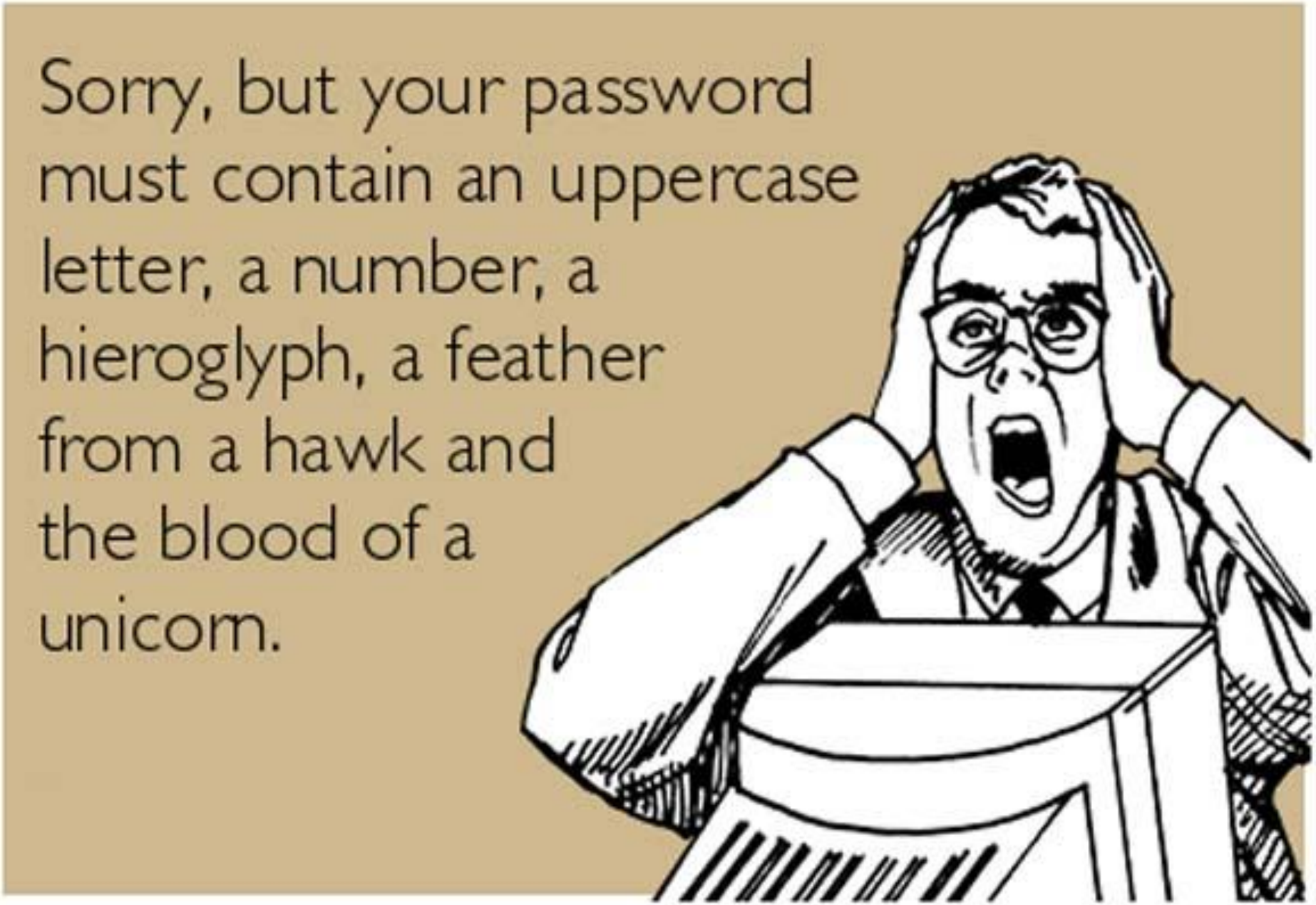
@itrjwyss

Oracle
Groundbreaker
Ambassador



@itrjwyss

AMBASSADOR



Oracle Groundbreaker Ambassador

ENTER PASSWORD
CLICK CLACK
WRONG PASSWORD
WRONG PASSWORD
WRONG PASSWORD
WRONG PASSWORD
RESET YOUR PASSWORD
WRONG PASSWORD
ENTER YOUR NEW PASSWORD
ENTER YOUR NEW PASSWORD
YOUR NEW PASSWORD CANNOT BE YOUR OLD PASSWORD
CHARLOTTE GOMEZ/BUZZFEED

AMBASSADOR

ENTER PASSWORD
CLICK CLACK
WRONG PASSWORD
WRONG PASSWORD
WRONG PASSWORD
WRONG PASSWORD
RESET YOUR PASSWORD
WRONG PASSWORD
ENTER YOUR NEW PASSWORD
ENTER YOUR NEW PASSWORD
YOUR NEW PASSWORD CANNOT BE YOUR OLD PASSWORD

AMBASSADOR

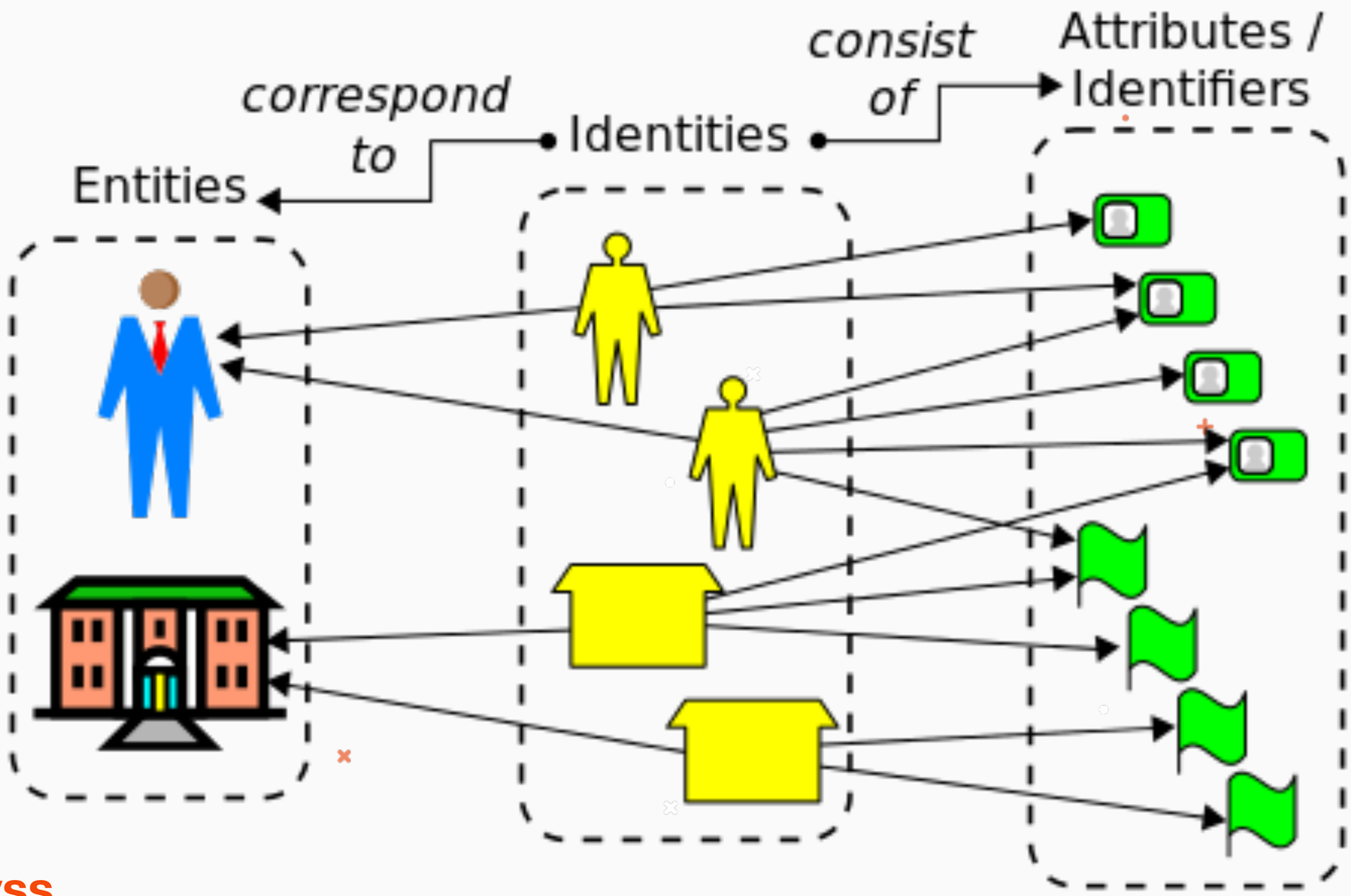
What we can do to improve this process? Making it safer and easier.

Identity Management (IdM)

- Is an umbrella term for all of the core logic around identity in a corporate environment.
  - Provisioning
  - Account management
  - Identity governance

AMBASSADOR

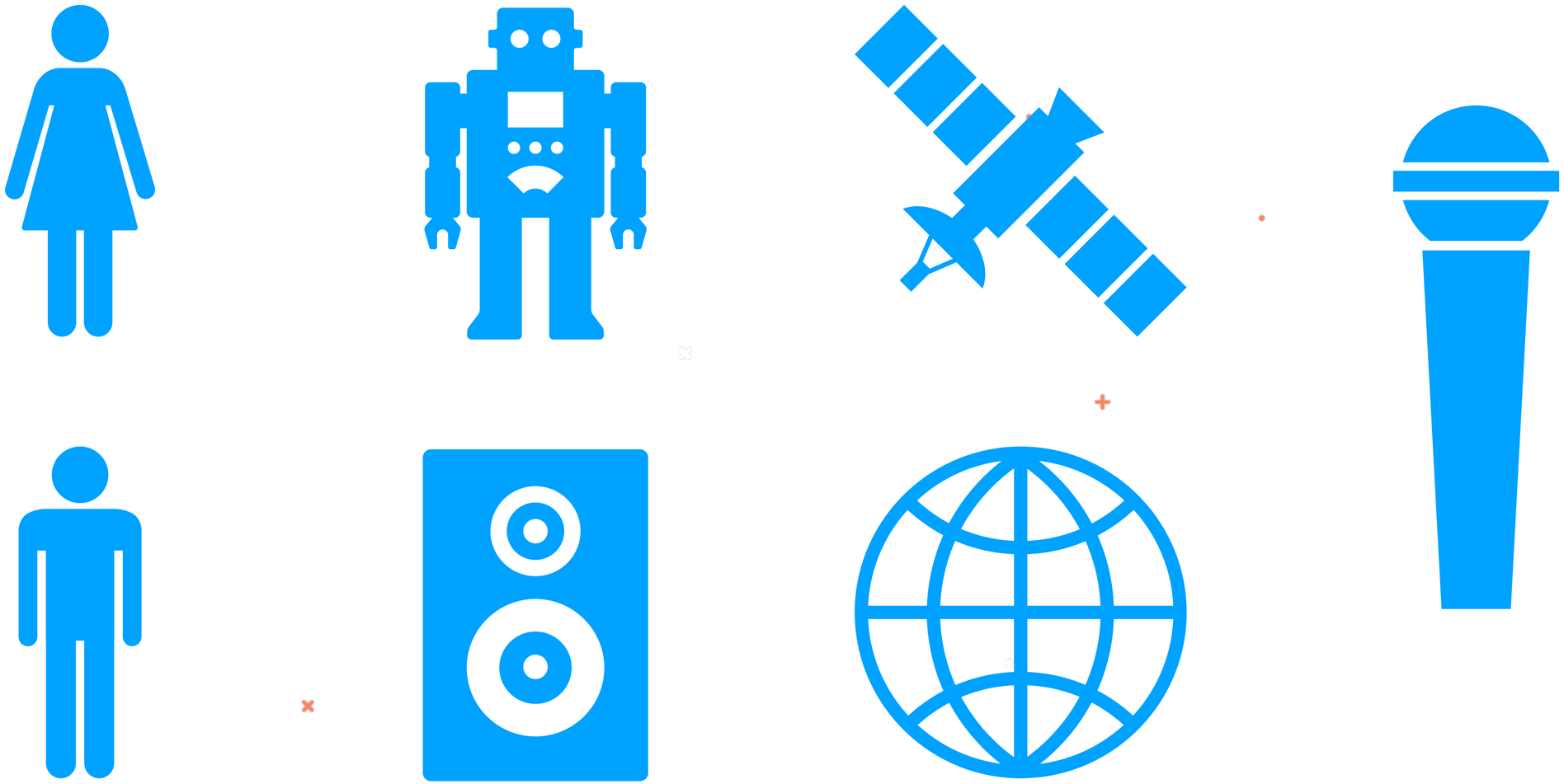
IdM: Provisioning



@itrjwyss

Oracle Groundbreaker Ambassador

IdM: Provisioning



@itrjwyss

IdM: Account Management

- Maintain those identities
- How safe those data?
- Encryption, Which one, which keys?
- What happens when an Entity erase their account?
- What happens when an Entity is longer inactive?

IdM: Identity Governance

- Assigning them to groups and roles and adjusting permissions as needed

@itrjwyss

Identity and Access Management (IAM)

- Is most often used to refer not just to identification, but to the whole suite of practices that a corporation needs to manage their users and data:
  - Authentication
  - Authorization
  - Identity Federation

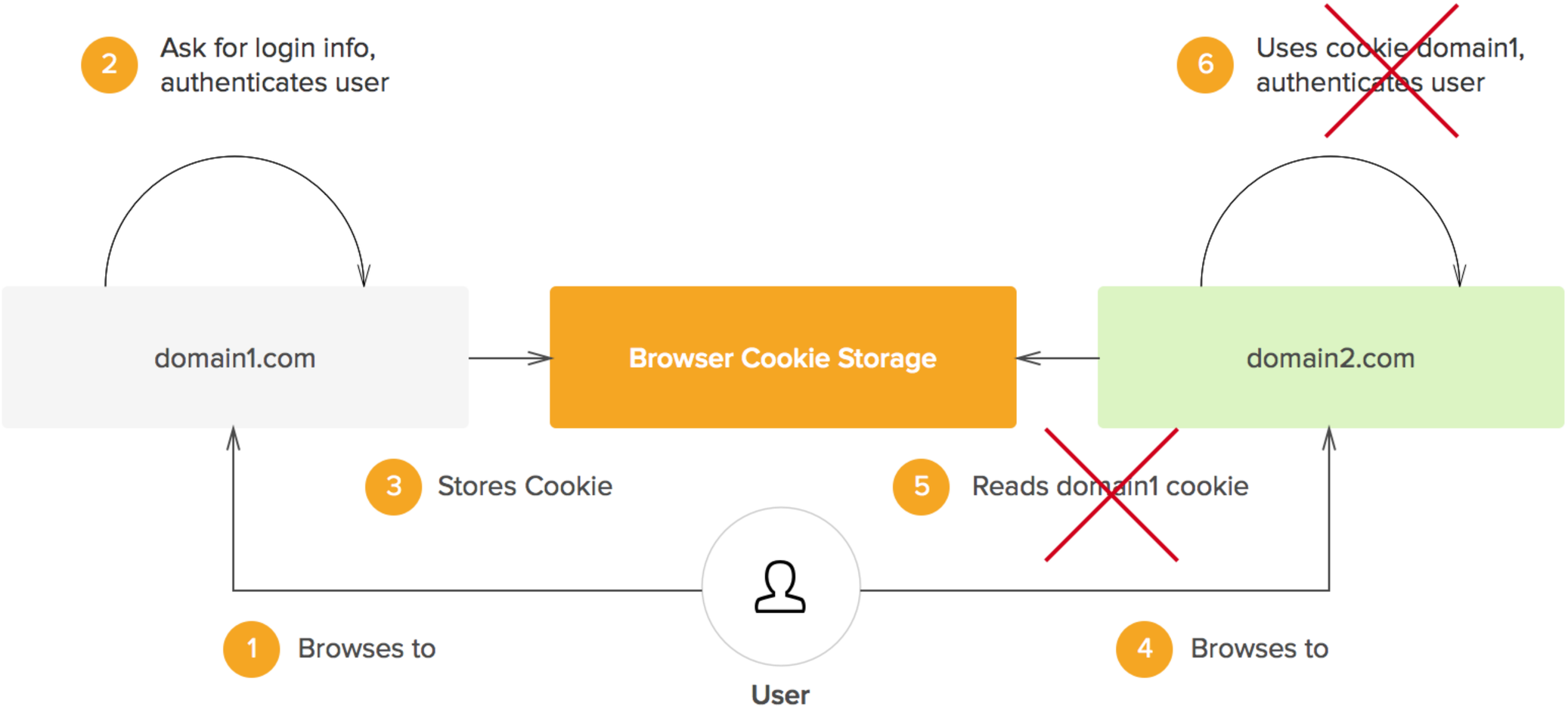
IAM: Authorization

- Ensuring the given user has the proper ***permissions to access*** a certain piece of data.

IAM: Identity Federation

- Ensuring users can use the same identification data to access resources on related domains.

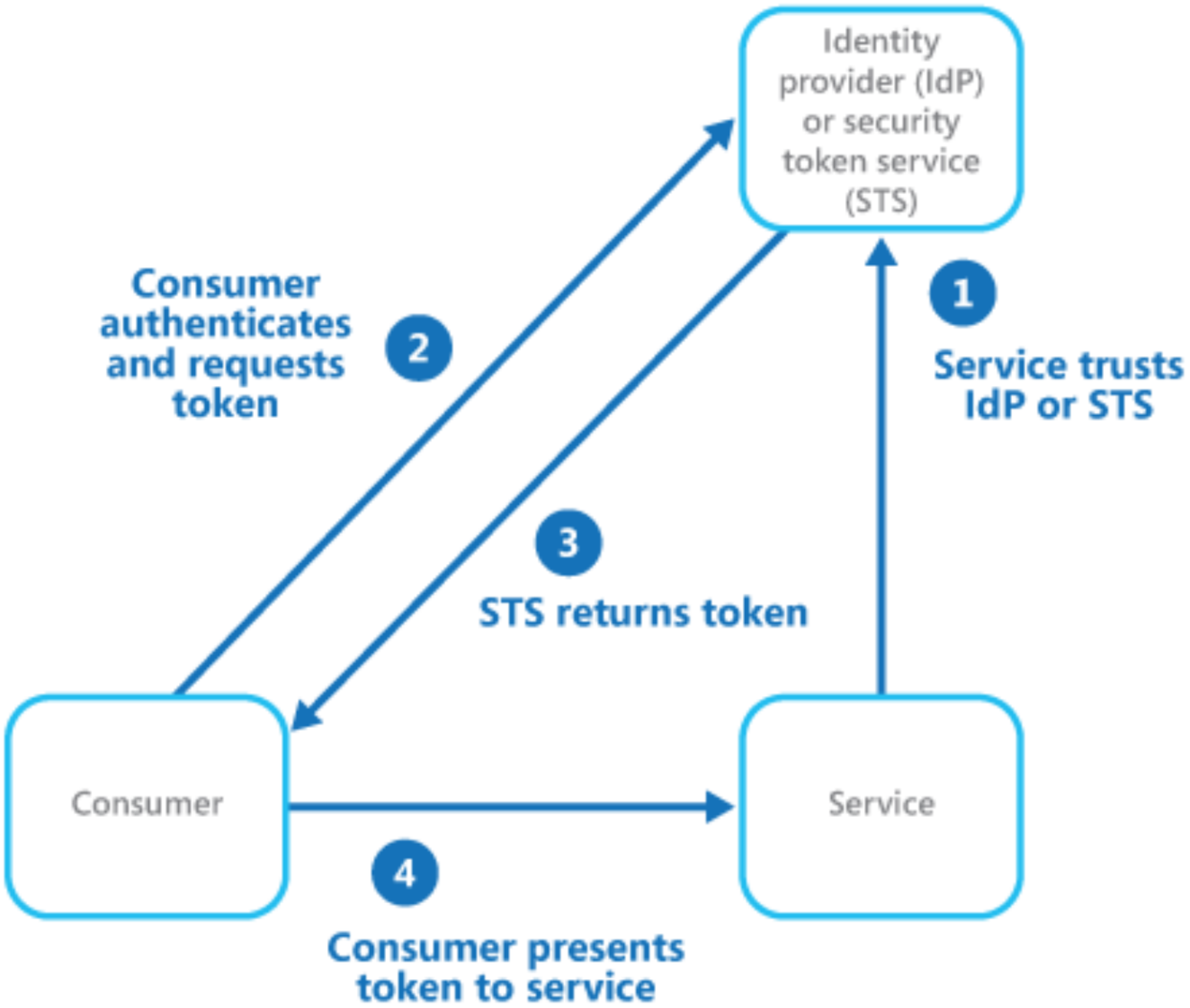
SAME-ORIGIN-POLICY FORBIDS THIS



@itrjwyss

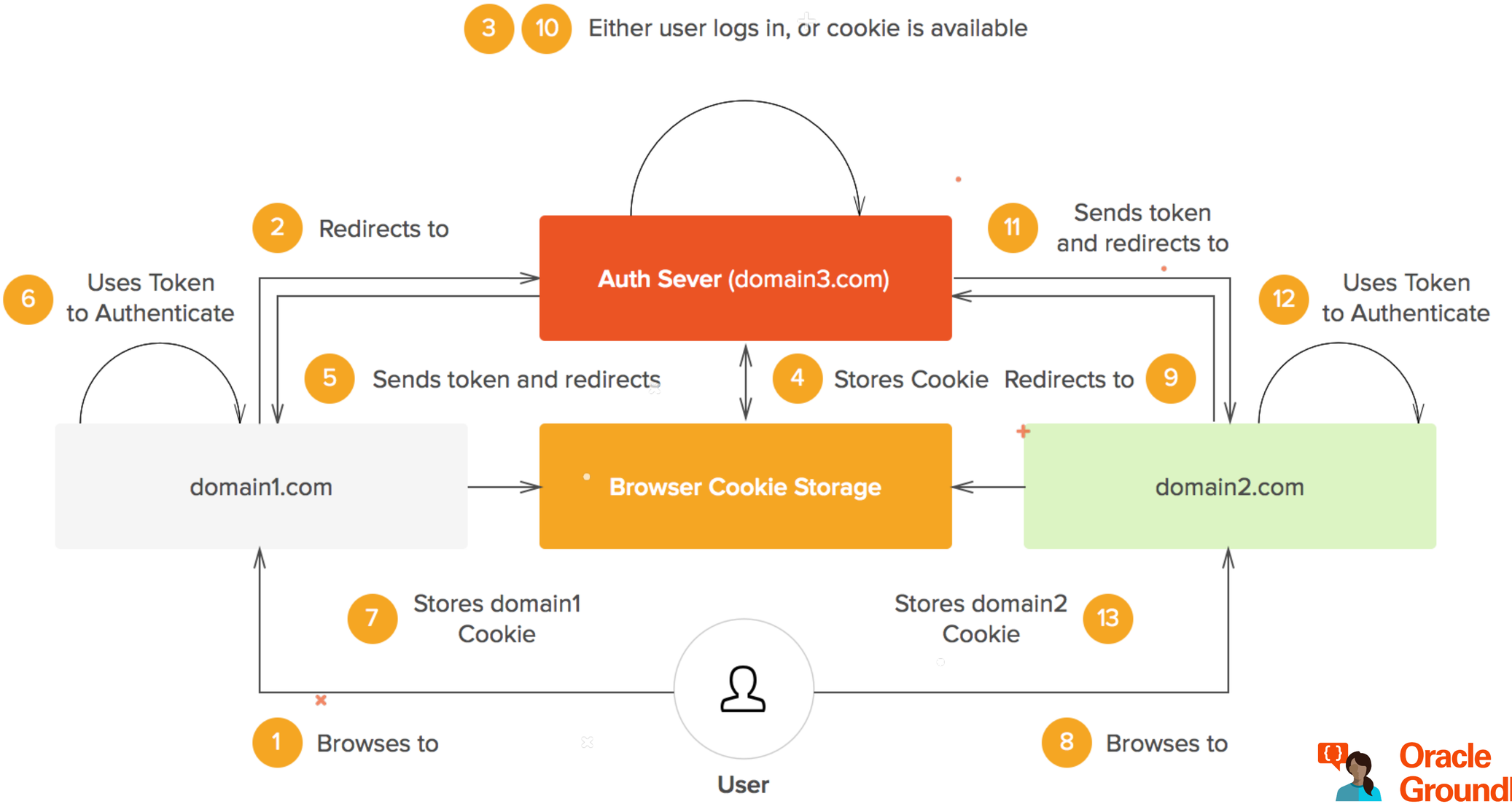
Federated Identity

- In some way, are methods of transferring data without violating the same origin policy.
- This way, if domain X and Y are related, and their owners want users to move freely between the two, they can simply triangulate around an external authorization server.


Identity provider (IdP) or security token service (STS)
1
Service trusts IdP or STS
Consumer authenticates and requests token
2
3
STS returns token
Consumer
Service
4
Consumer presents token to service

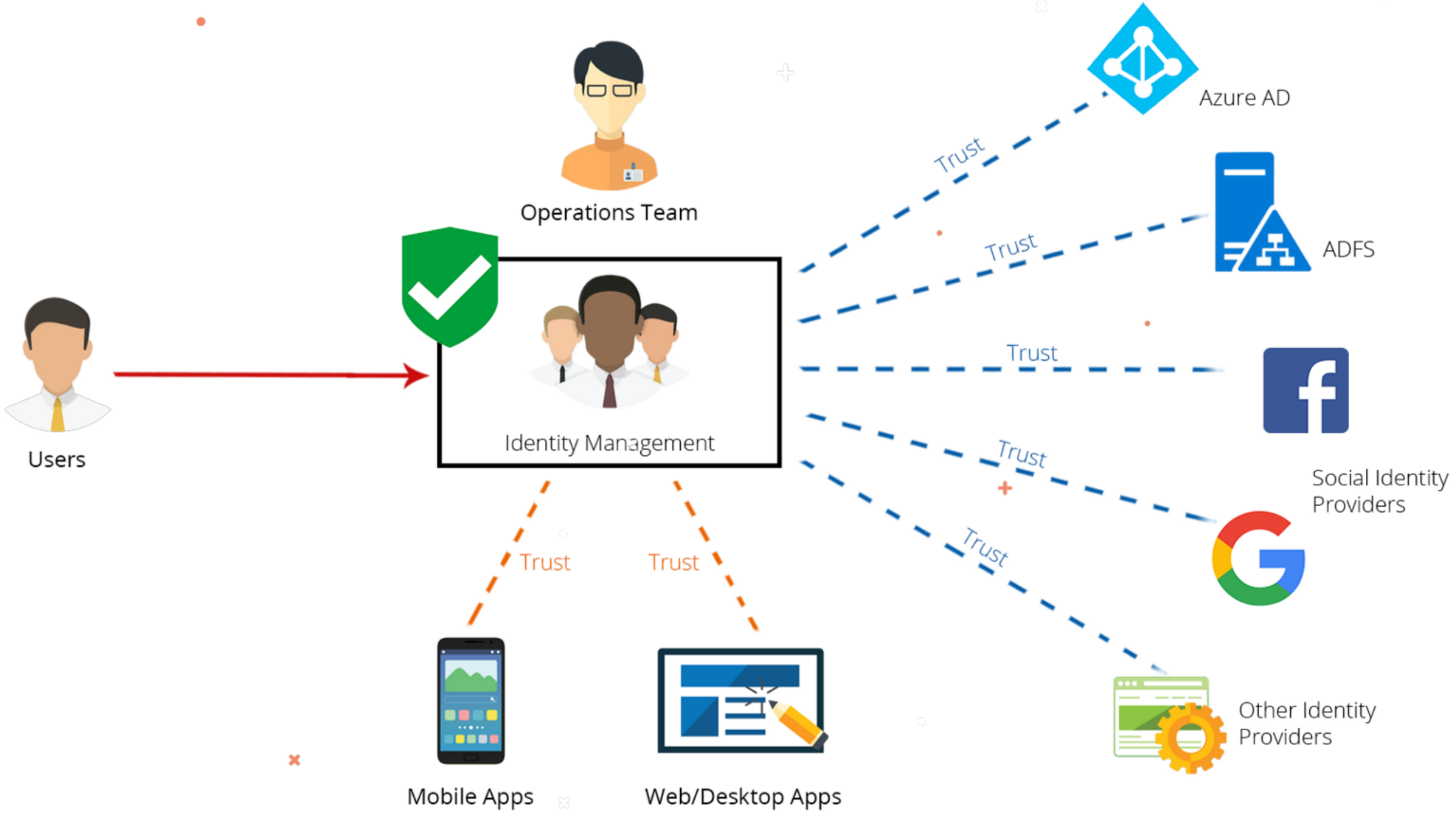
@itrjwyss

TYPICAL SSO



@itr

Oracle Groundbreaker Ambassador


Operations Team
Azure AD
Trust
Trust
ADFS
Users
Identity Management
Trust
Trust
Social Identity
Providers
Trust
Trust
Trust
Mobile Apps
Web/Desktop Apps
Other Identity
Providers

@itrjwyss

IAM: Authentication

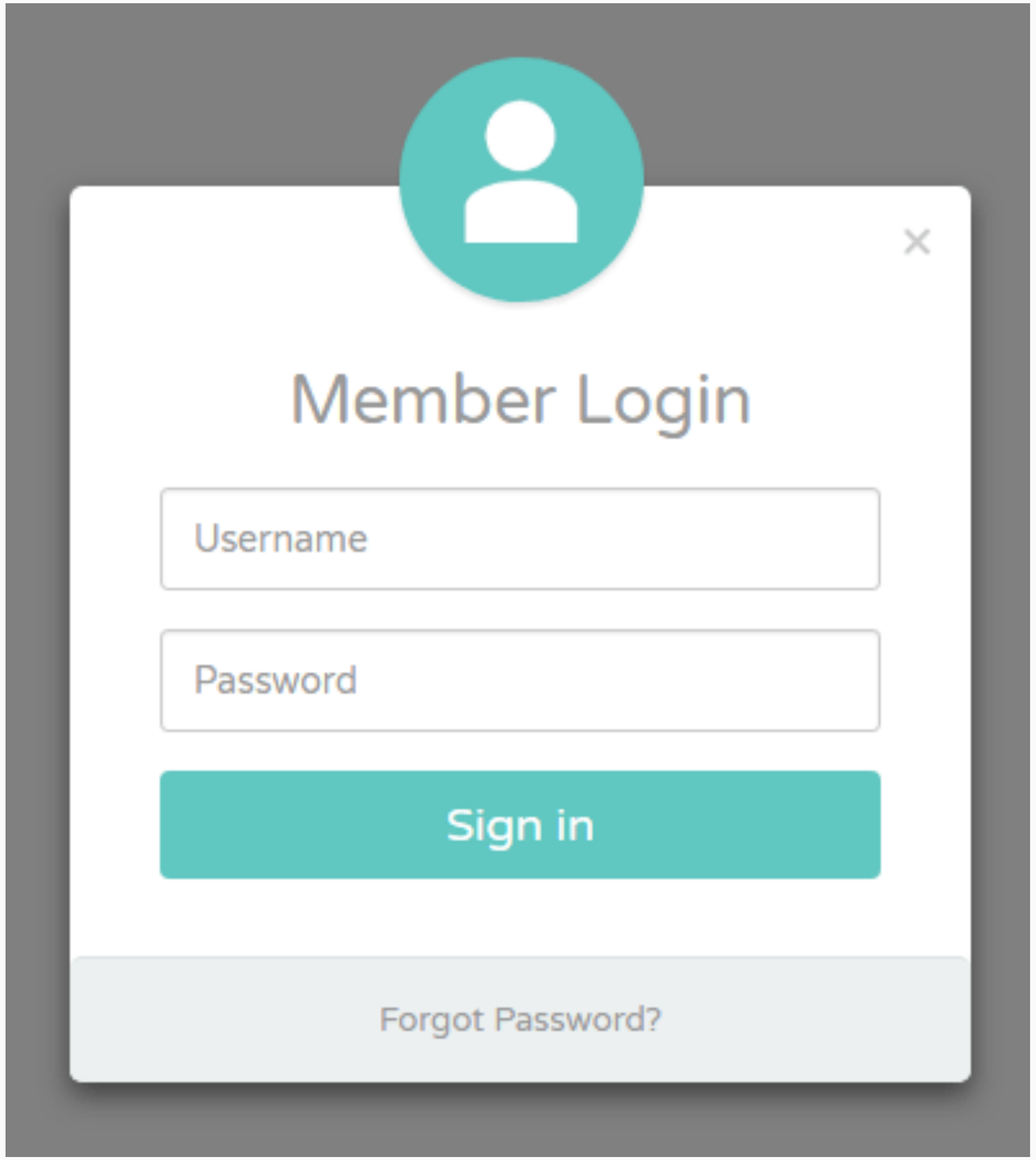
- Ensuring that a given user is the user they identify as
  - Single Sing On (SSO)
  - Multi-factor Authentication (MFA)
  - Passwordless

Knowledge

Possession

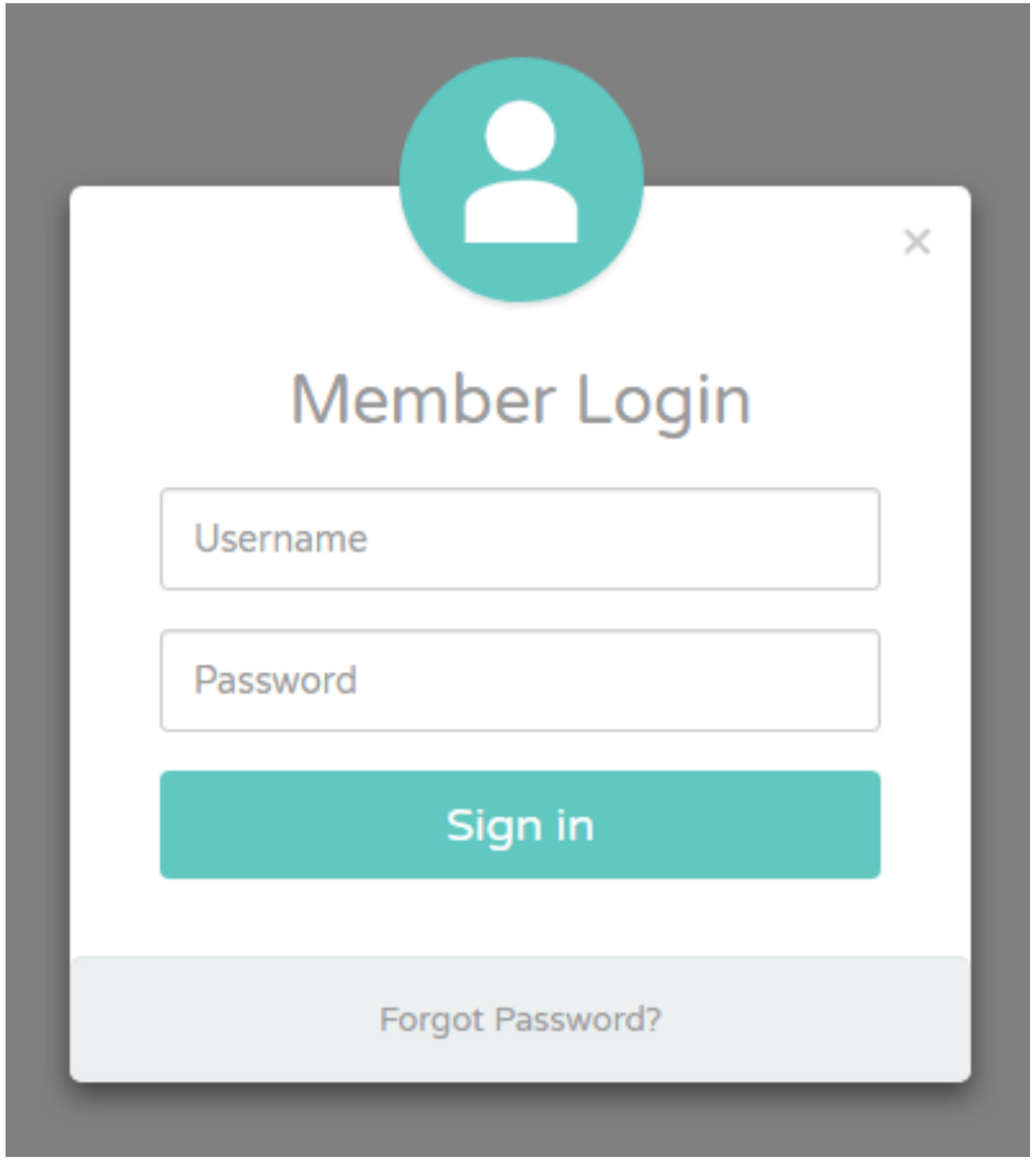
Biometric

@itrjwyss



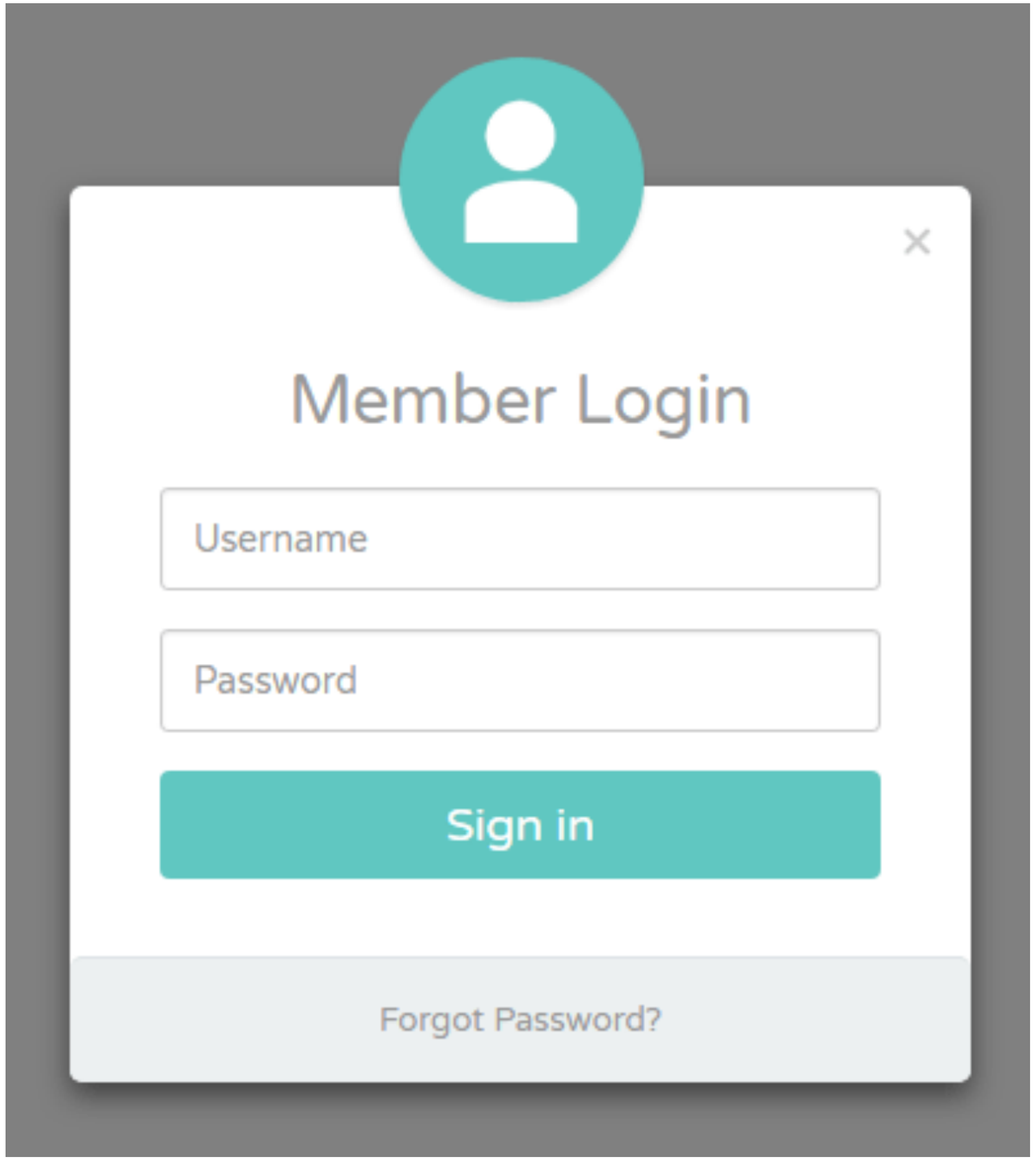
@itrjwyss

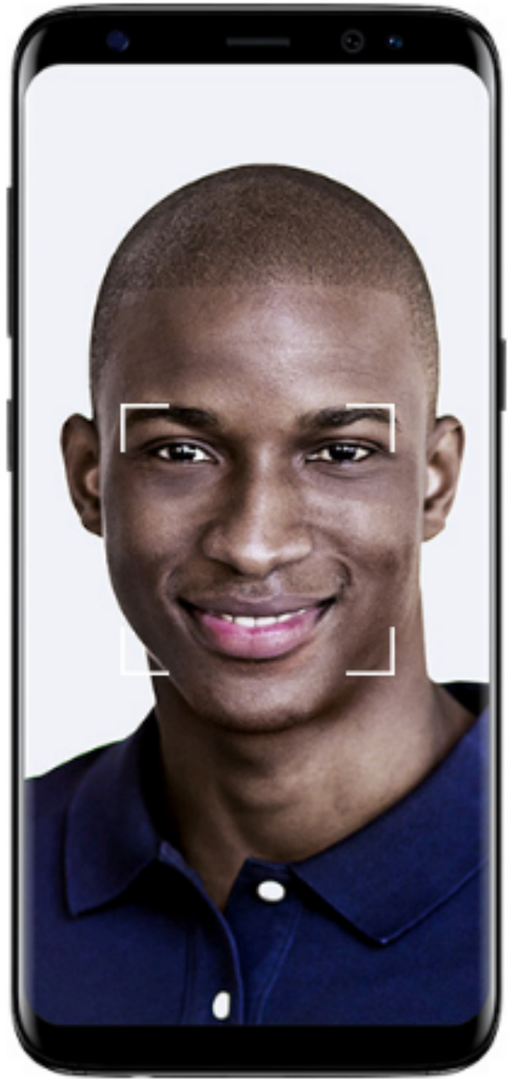
Oracle
Groundbreaker
Ambassador



@itrjwyss

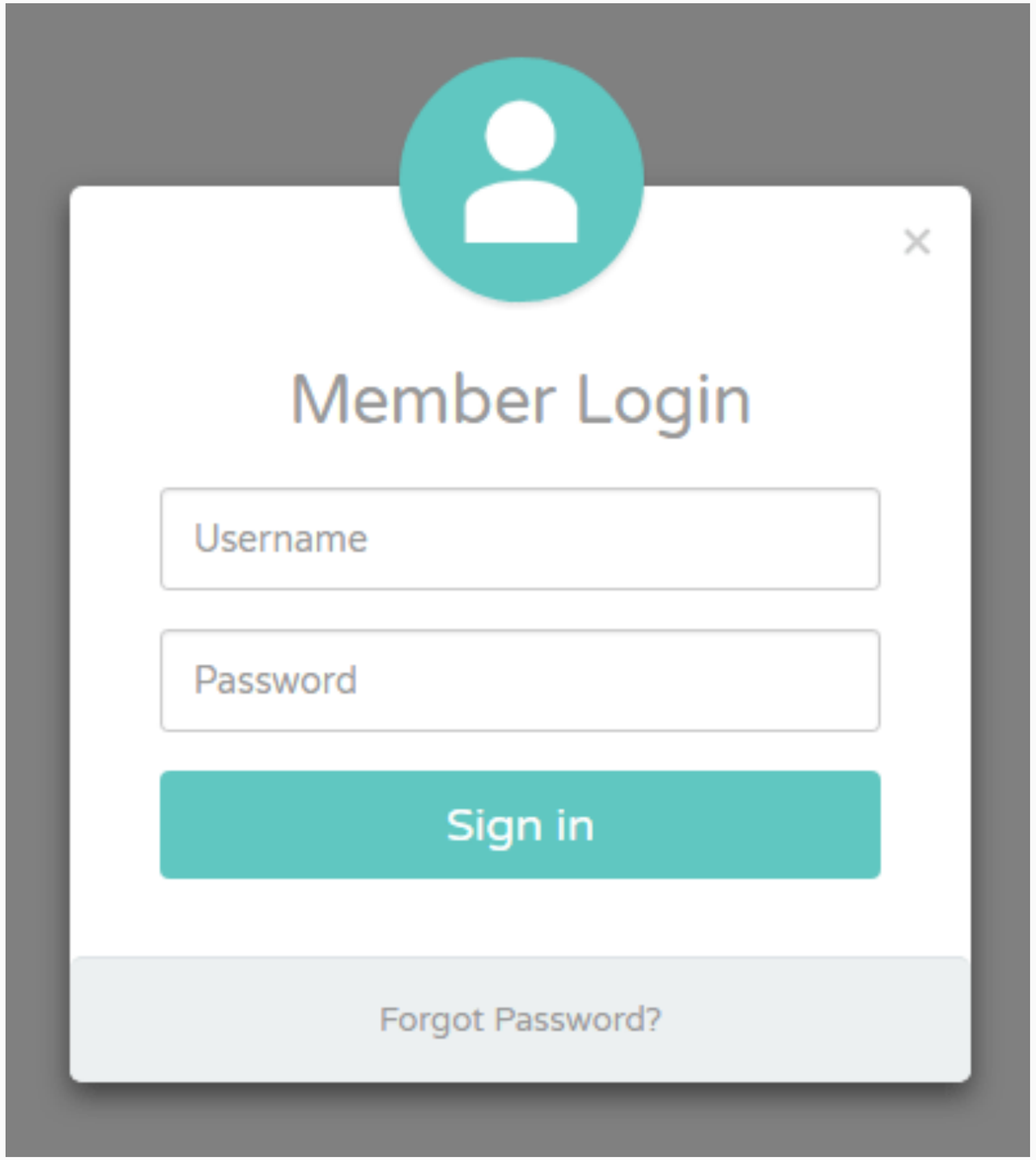
Oracle
Groundbreaker
Ambassador





@itrjwyss

Oracle Groundbreaker Ambassador



@itrjwyss

Oracle
Groundbreaker
Ambassador

MFA

Multi-Factor Authentication

@itrjwyss

AMBASSADOR

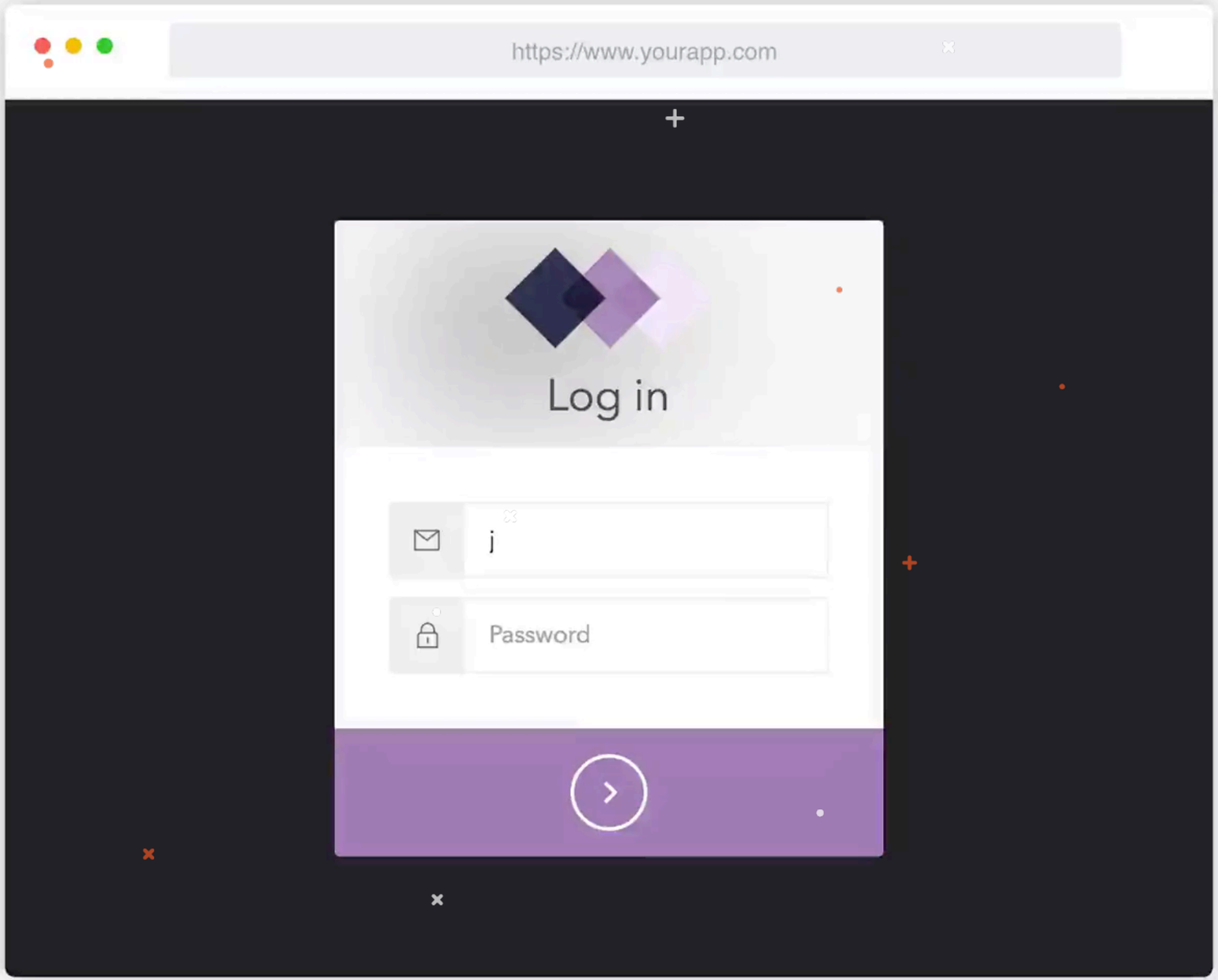
User logs into an account using their primary password

An authentication code (OTP) is sent to the user's mobile phone

User enters the OTP as the secondary password and is granted access to their online account

@itrjwyss

Oracle Groundbreaker Ambassador

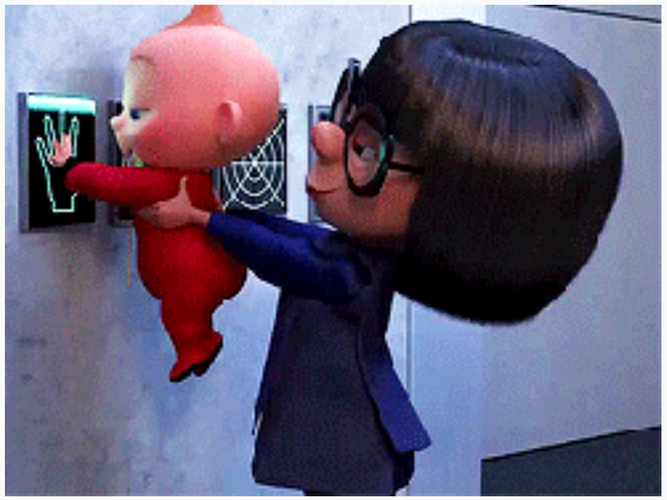

https://www.yourapp.com
Log in
j
Password

MFA: Biometrics

- Common methods are touch ID (fingerprint), SMS, facial recognition.
- We can have other ones:
    - Iris or retina recognition
    - Voice recognition (Twilio)
    - Typing recognition
    - DNA usage

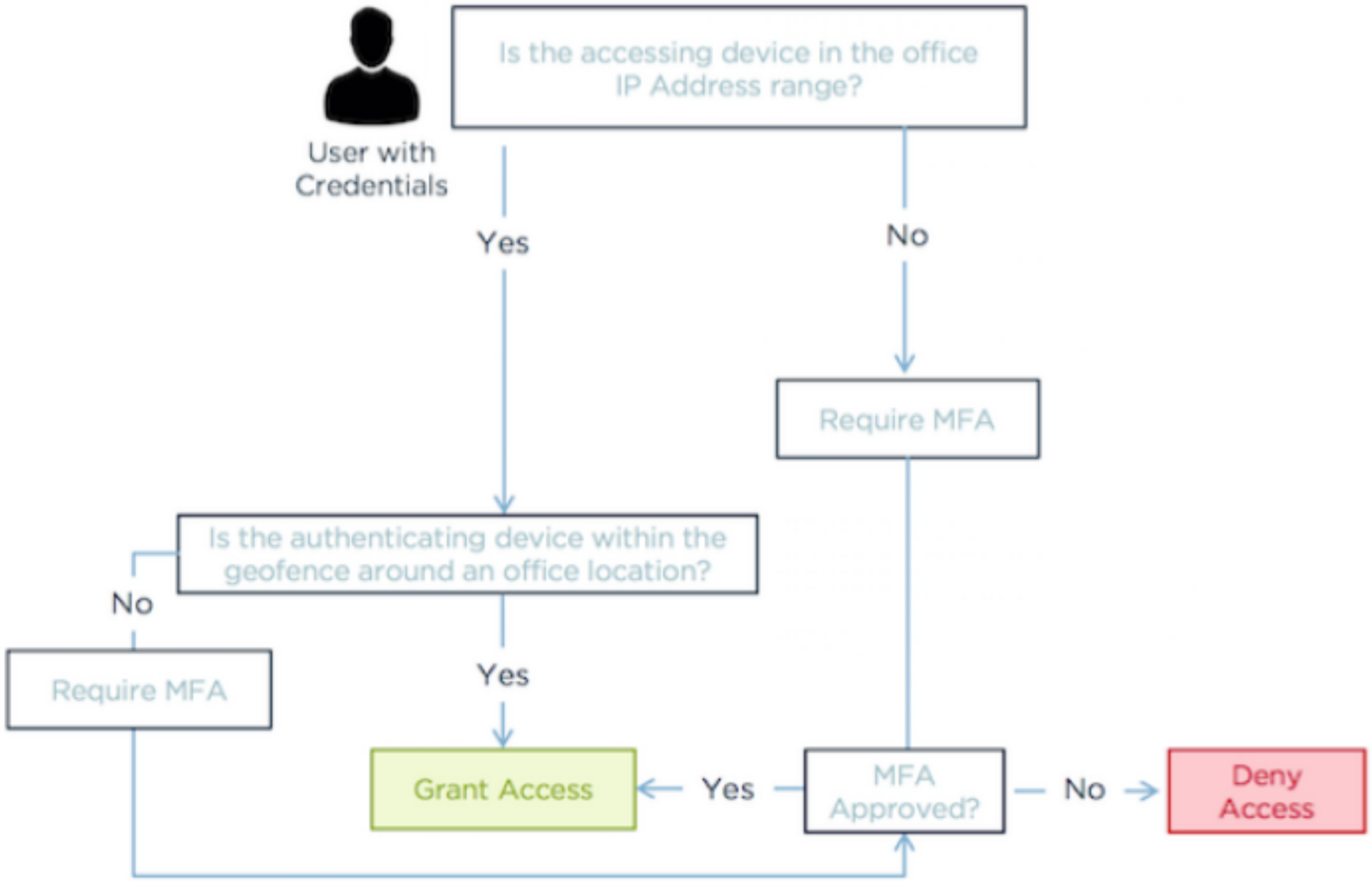
MFA: Biometrics

- Common methods are touch ID (fingerprint), SMS, facial recognition.
- We can have other ones:
  - Iris or retina recognition
  - Voice recognition (Twilio)
  - Typing recognition
  - DNA usage



Passwordless

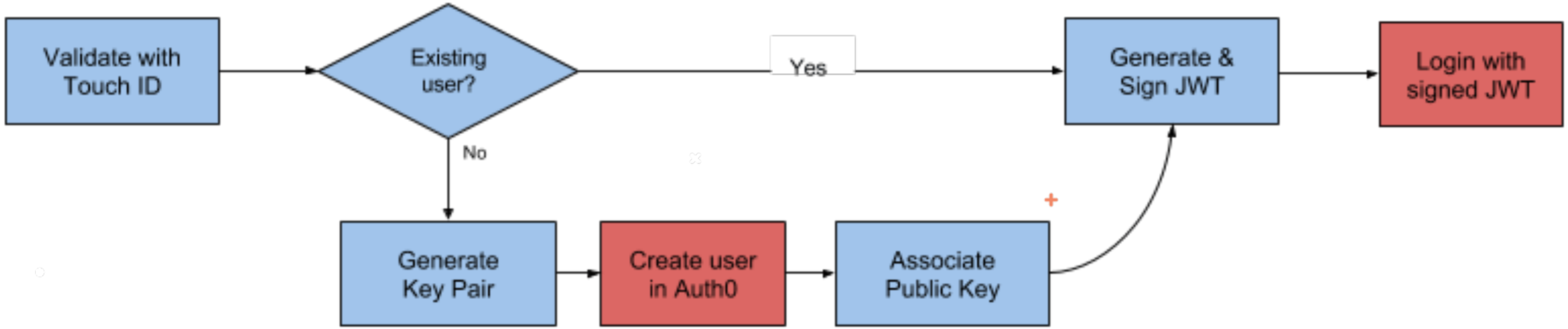
- It means authenticating a user by means other than having them type in a password
- Can also evaluate user and device contexts to provide authentication methods.



@itrjwyss

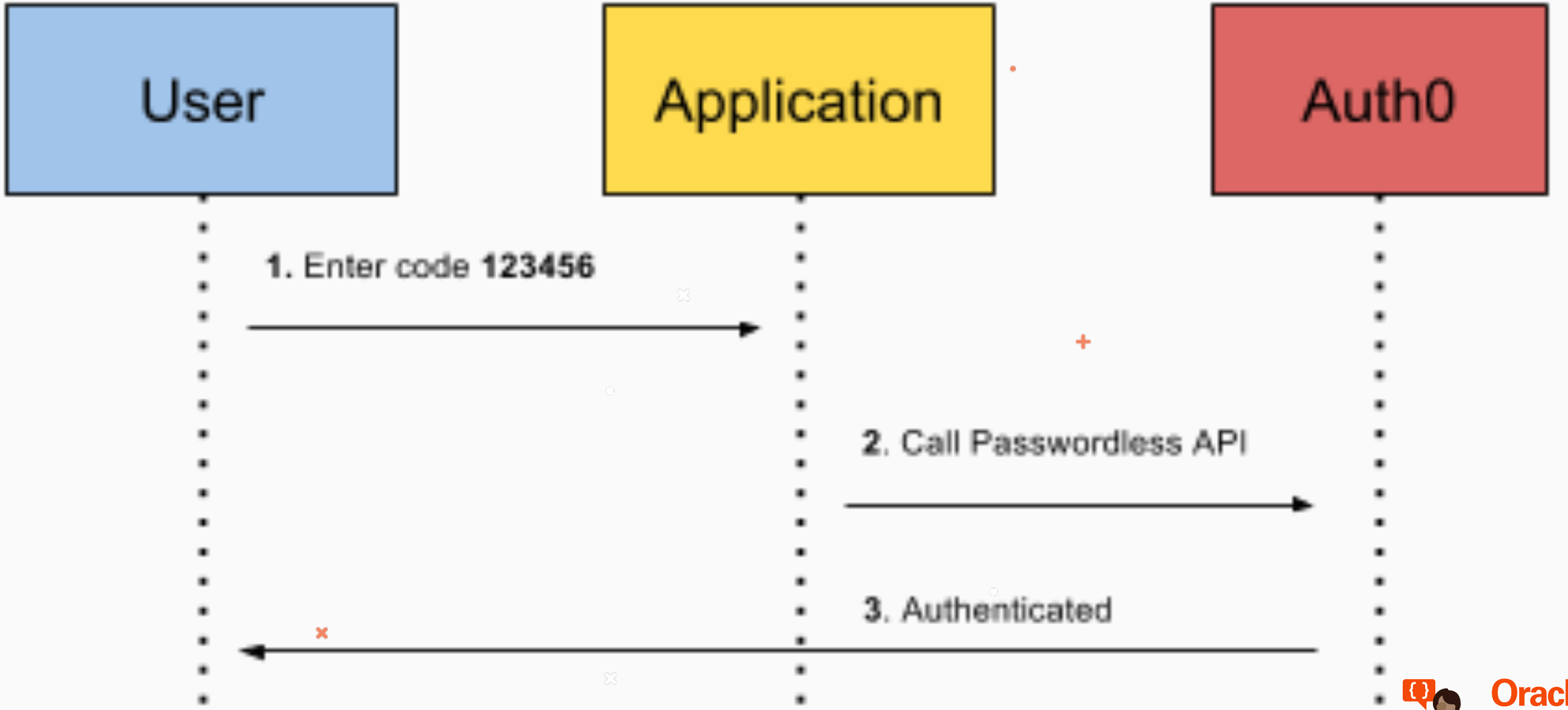
Oracle Groundbreaker Ambassador

Touch ID



@itrjwyss

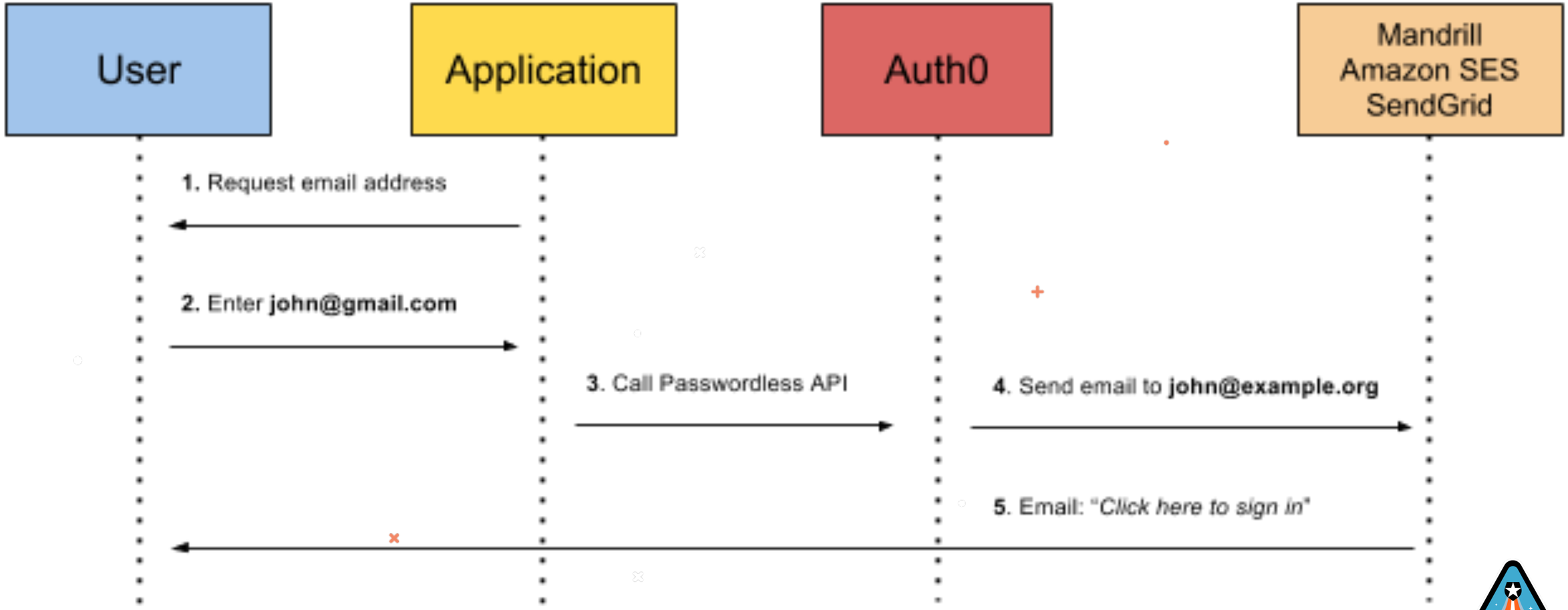
SMS Code



@itrjwyss

Oracle Groundbreaker Ambassador

Magic Link



@itrjwyss

slack

@itrjwyss

Oracle
Groundbreaker
Ambassador

slack

Hello!

You asked us to send you a magic link for quickly signing in to raywenderlich.com, using the app. Your wish is our command! ✨

Sign in to Slack

You may copy/paste this link into your browser:
https://app.slack.com/t/raywenderlich/login/z-app-2702402525-227951624851-ZuEuoyDoA8?s=slack&x=x-207503661156-229118386967

Note: Your magic link will expire in 24 hours, and can only be used one time.

See you soon!

Cheers,
The team at Slack

@itrjwyss

AMBASSADOR

Social Federated Identity

@itrjwyss

Oracle Groundbreaker Ambassador

Basecamp

Amazon Web Services

AOL Reader

Auth0 OpenIDConnect

Baidu

Bitbucket

Box

Docomo

@itrjwyss

AMBASSADOR

Dropbox

Dwolla

Evernote

Exact

Facebook

Fitbit

Github

Goodreads

Google

Instagram

LinkedIn

Microsoft Account

miiCard

Generic OAuth2 Provider

PayPal

Planning Center

@itrjwyss

AMBASSADOR

RenRen

Salesforce

Shopify

SoundCloud

The City

Twitter

vKontakte

Weibo

@itrjwyss

Oracle
Groundbreaker
Ambassador

WordPress

Yahoo!

Yammer

Yandex

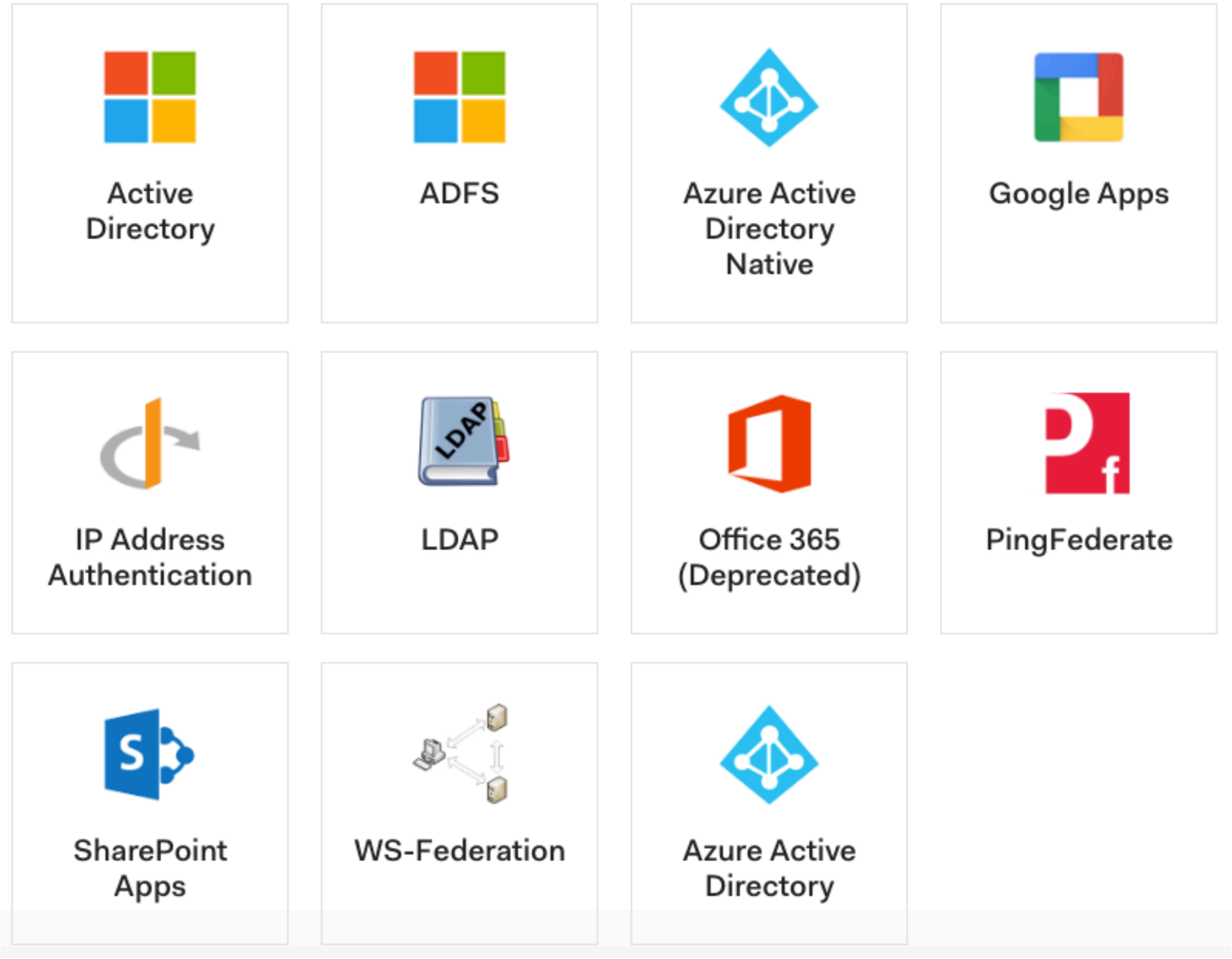
@itrjwyss

AMBASSADOR

Enterprise Federated Identity

@itrjwyss

Oracle
Groundbreaker
Ambassador


Active Directory
ADFS
Azure Active Directory Native
Google Apps
IP Address Authentication
LDAP
Office 365 (Deprecated)
PingFederate
SharePoint Apps
WS-Federation
Azure Active Directory

@itrjwyss

Legal Federated Identity

@itrjwyss

Oracle Groundbreaker Ambassador

bankID

Norwegian BankID

BankID

Swedish BankID

NEM ID

Danish NemID

@itrjwyss

AMBASSADOR

How to have a successful Identity Management Project

@itrjwyss

Oracle Groundbreaker Ambassador

Common Oversights and Pitfalls

- Identify requirements for the ***entire identity management lifecycle***, not just logging in
- Plan for identity failure and change, so you are ready for such events
- Address security and compliance requirements

1. How will user accounts be created?

@itrjwyss

Oracle Groundbreaker Ambassador

2. Will user profiles need to be synchronized?

@itrjwyss

AMBASSADOR

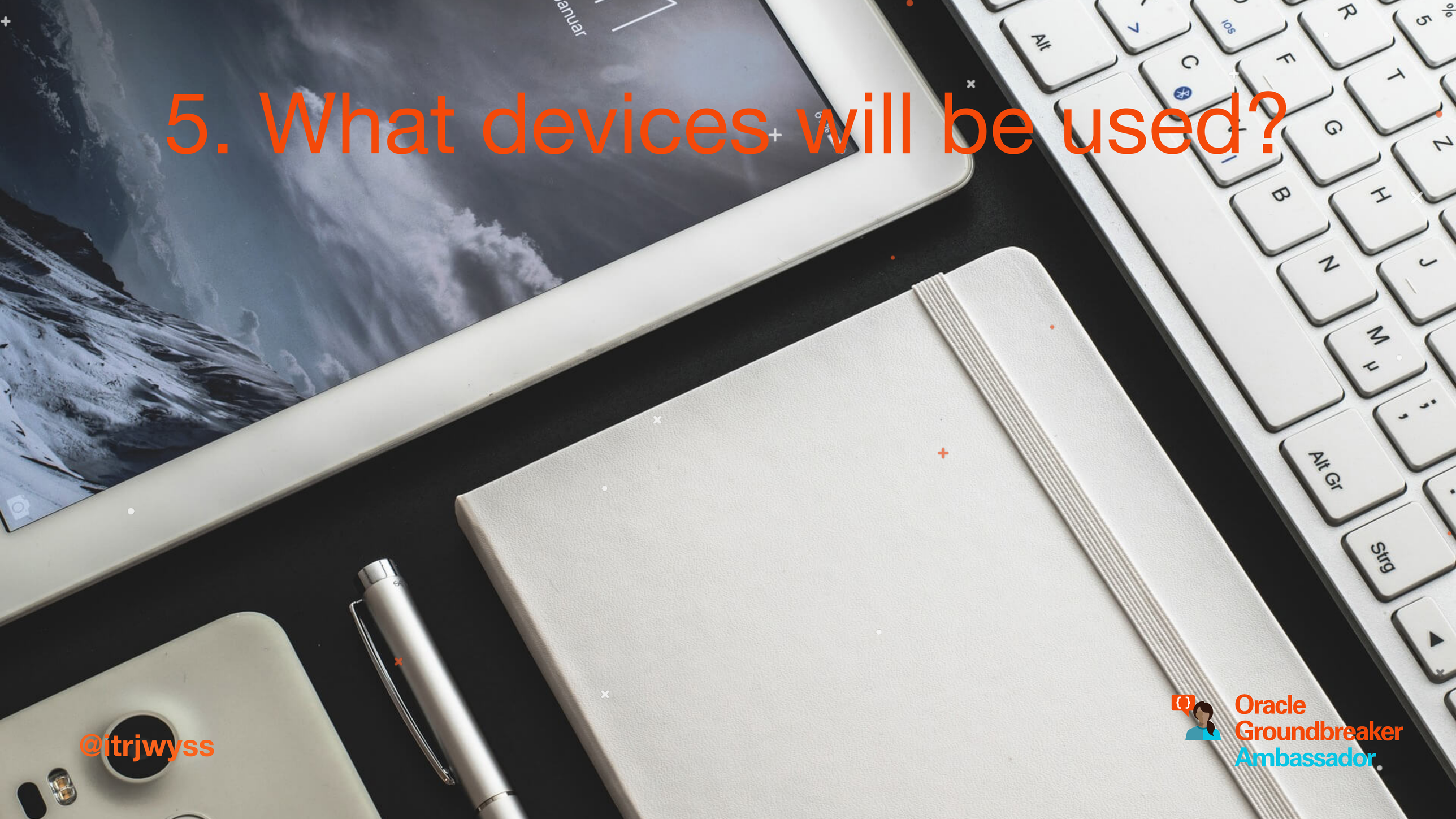
3. Username uniqueness

4. How will users Log In?

@itrjwyss

AMBASSADOR

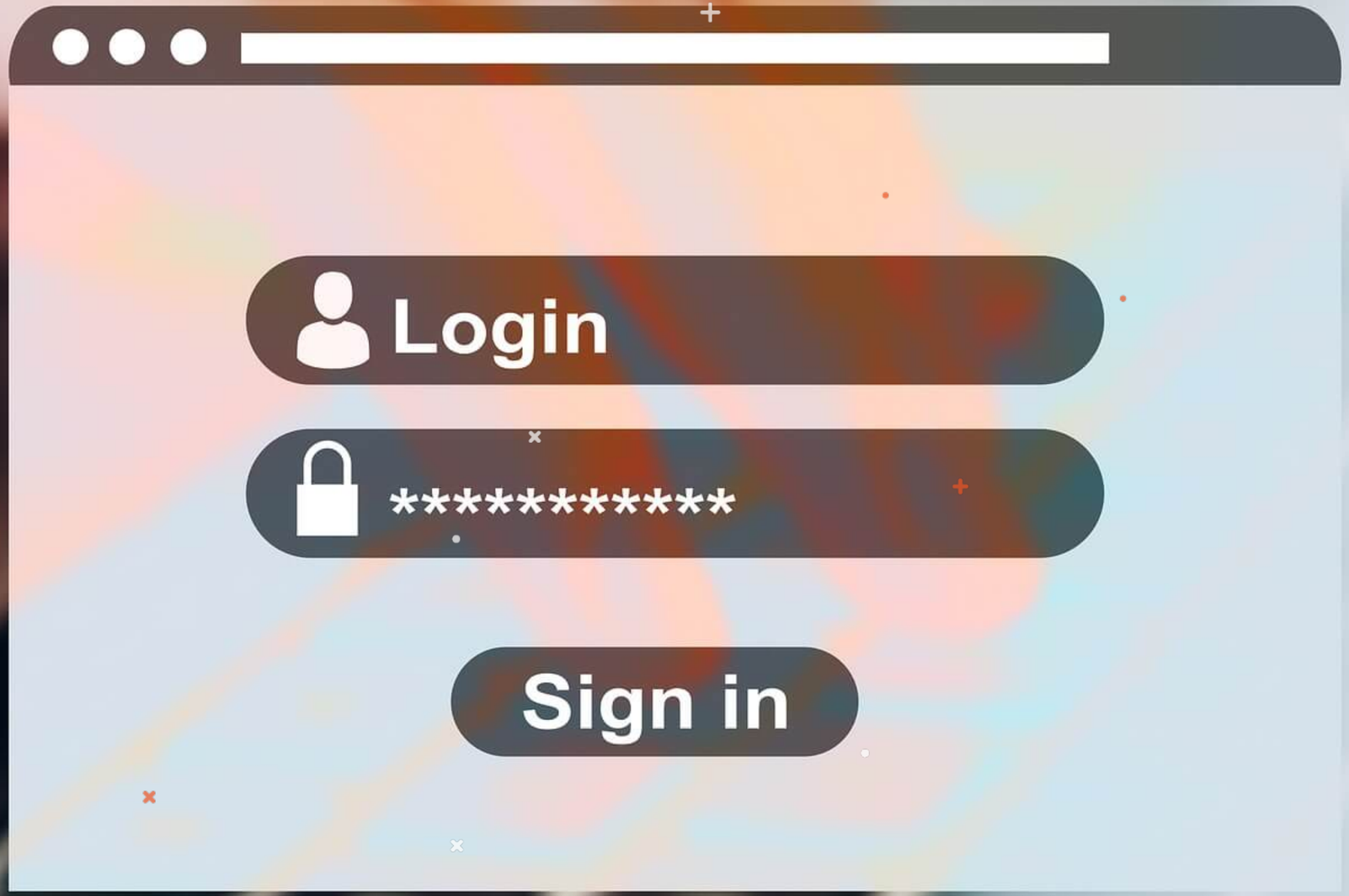
5. What devices will be used?



@itrjwyss

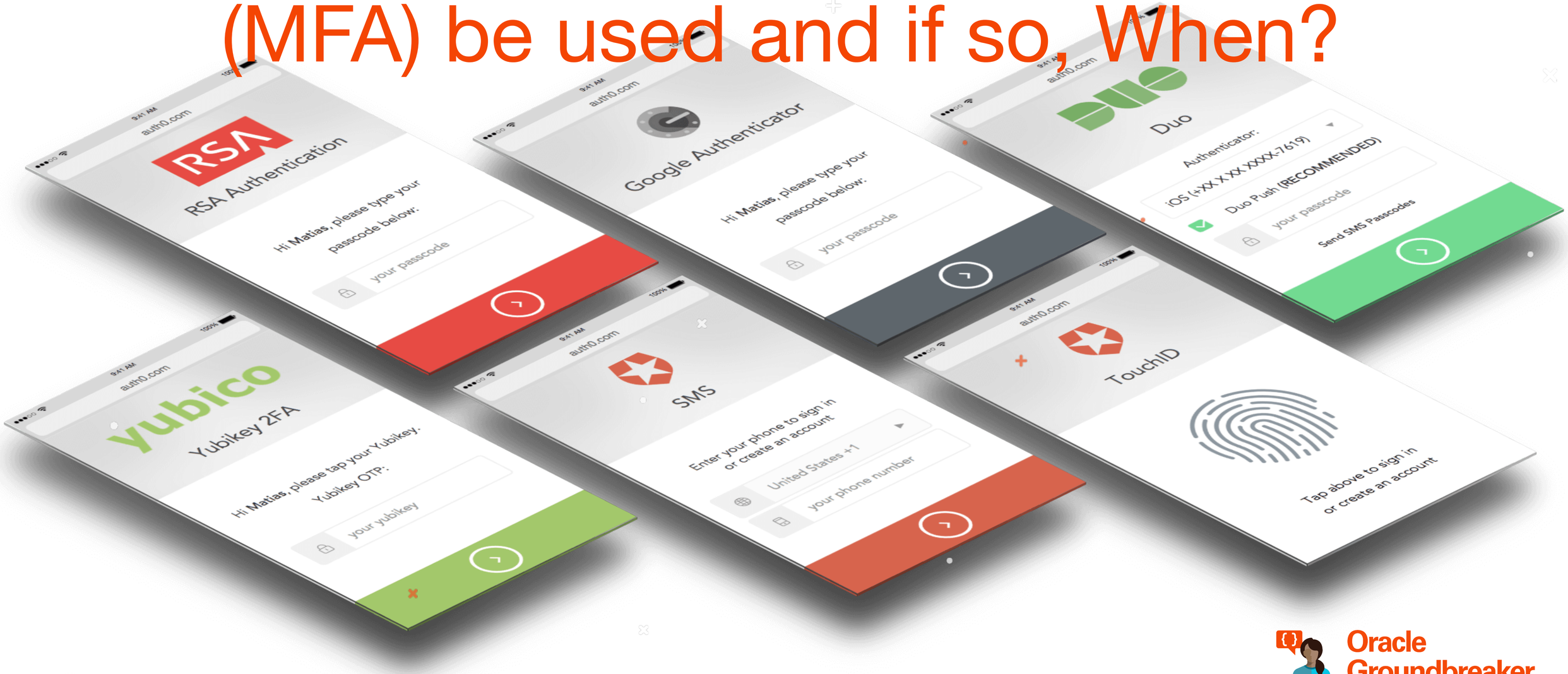
Oracle
Groundbreaker
Ambassador

6. Is single Sing-On needed?



@itrjwyss

7. Should Multi-Factor Authentication (MFA) be used and if so, When?



@itrjwyss

Oracle Groundbreaker Ambassador

8. What should happen when the User decides to Log Out?

@itrjwyss

9. How will browser configuration influence Sessions?

@itrjwyss

Oracle Groundbreaker Ambassador

10. Session Timeouts

@itrjwyss

11. Deprovisioning: What happens when it's over?

@itrjwyss

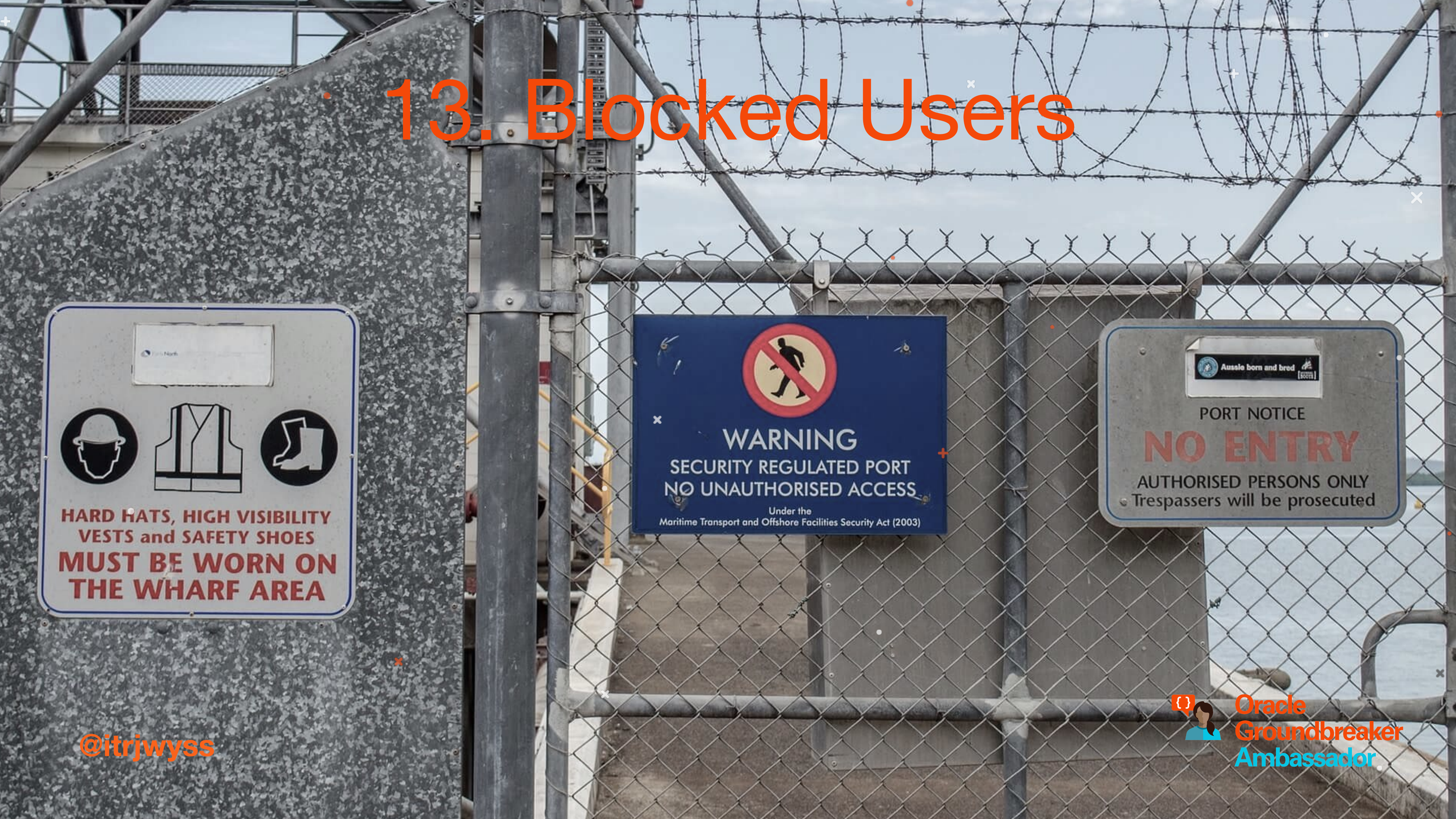
Oracle Groundbreaker Ambassador

12. Password Reset

@itrjwyss

AMBASSADOR

13. Blocked Users



@itrjwyss

Oracle
Groundbreaker
Ambassador

14. Anomaly Detection

@itrjwyss

14. Anomaly Detection

- A particular user having a large number of failed logins.
- A user logging in from two widely separated geographic locations within a short amount of time.
- Users whose credentials have been compromised and published on the internet in databases of hacked passwords, such as Troy Hunt's haveibeenpwned.

15. Privacy/Compliance requirements

@itrjwyss

AMBASSADOR

16. Audit Logs

@itrjwyss

Oracle Groundbreaker Ambassador

17. Consider how Identity Information might change over time

@itrjwyss

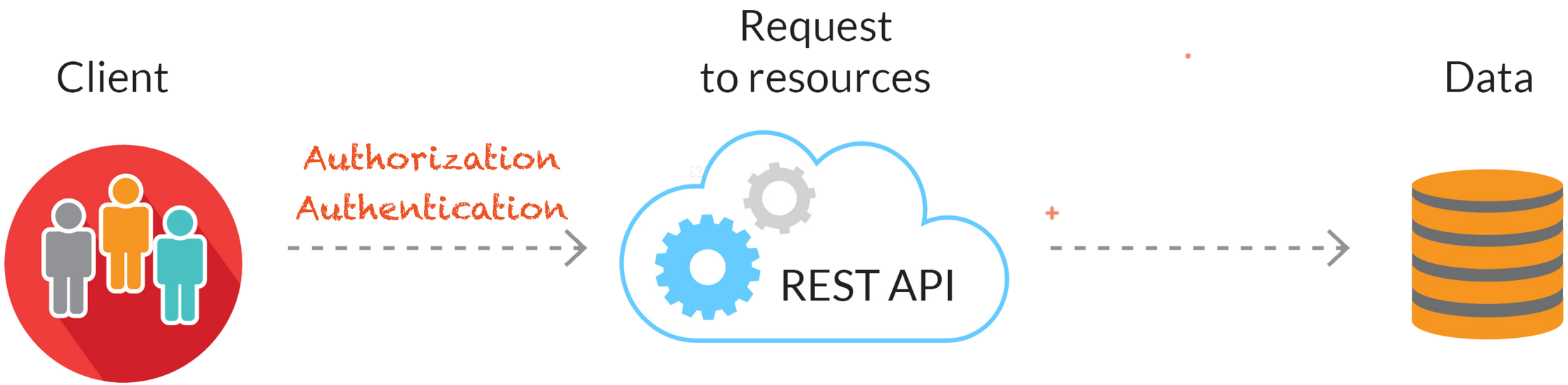
AMBASSADOR

What does this have to do with Serverless and Microservices?

@itrjwyss

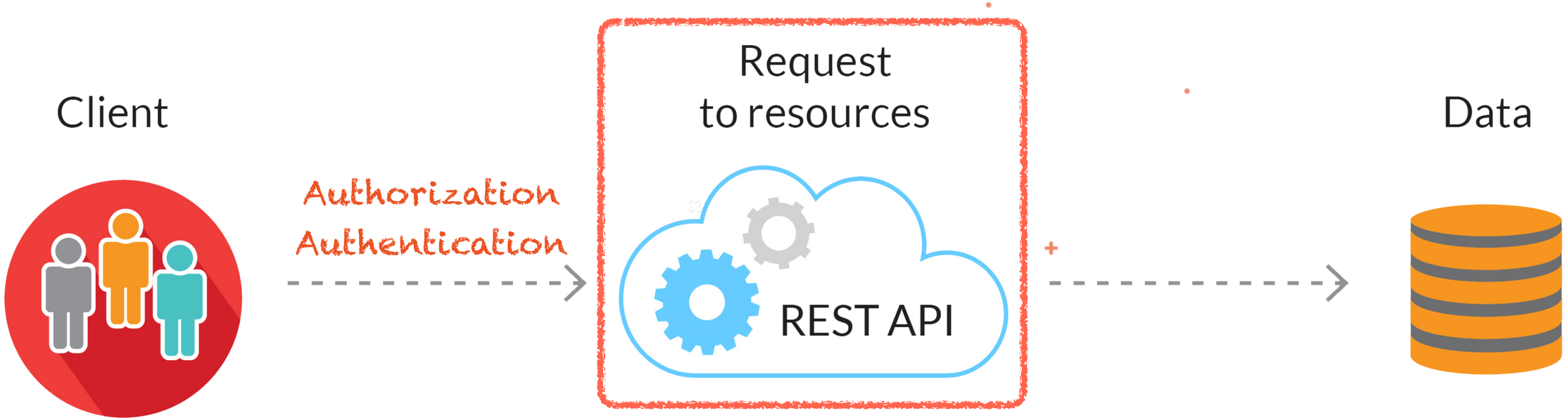
Oracle Groundbreaker Ambassador

Developing REST APIs

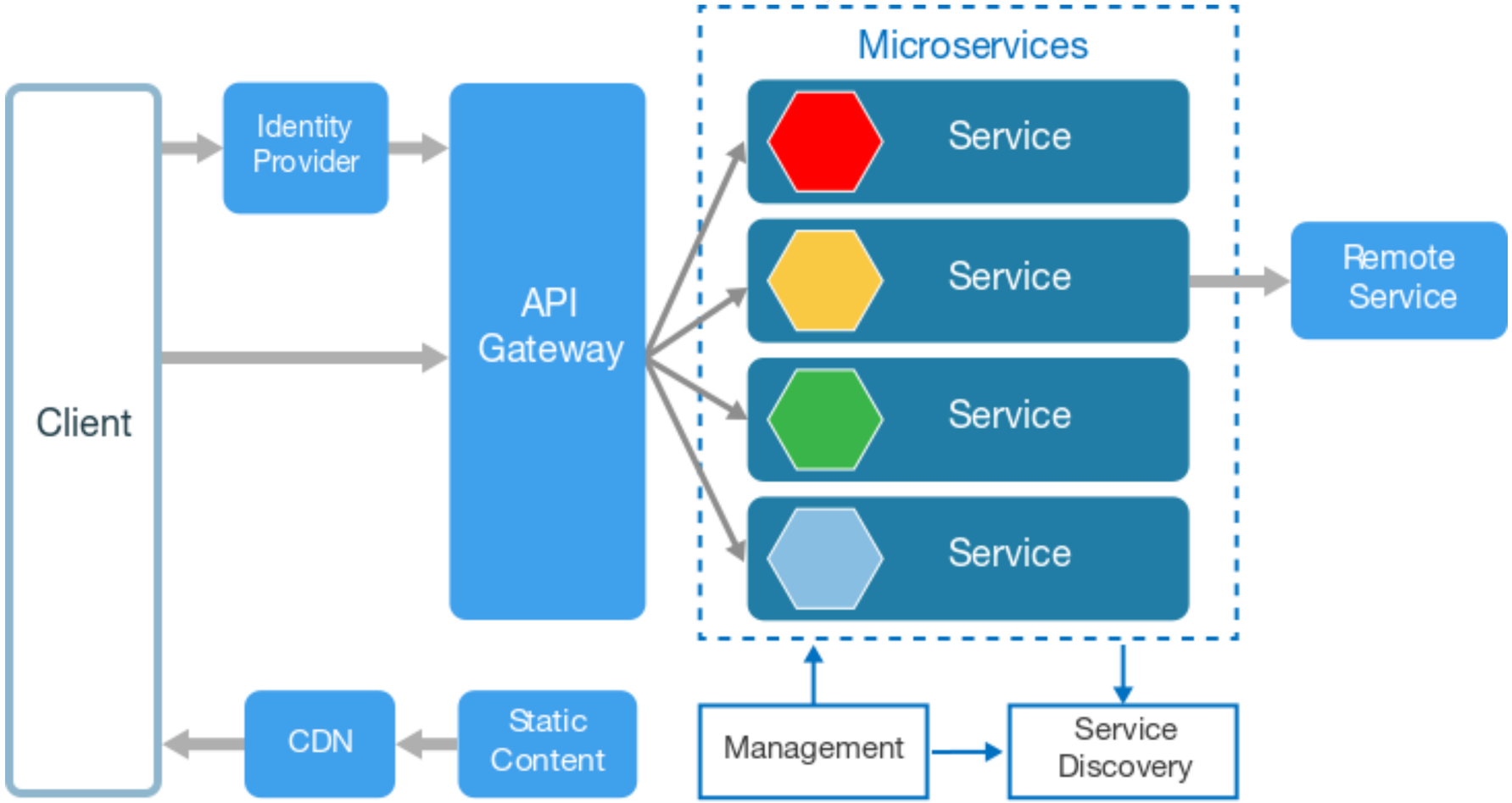


@itrjwyss

Developing REST APIs

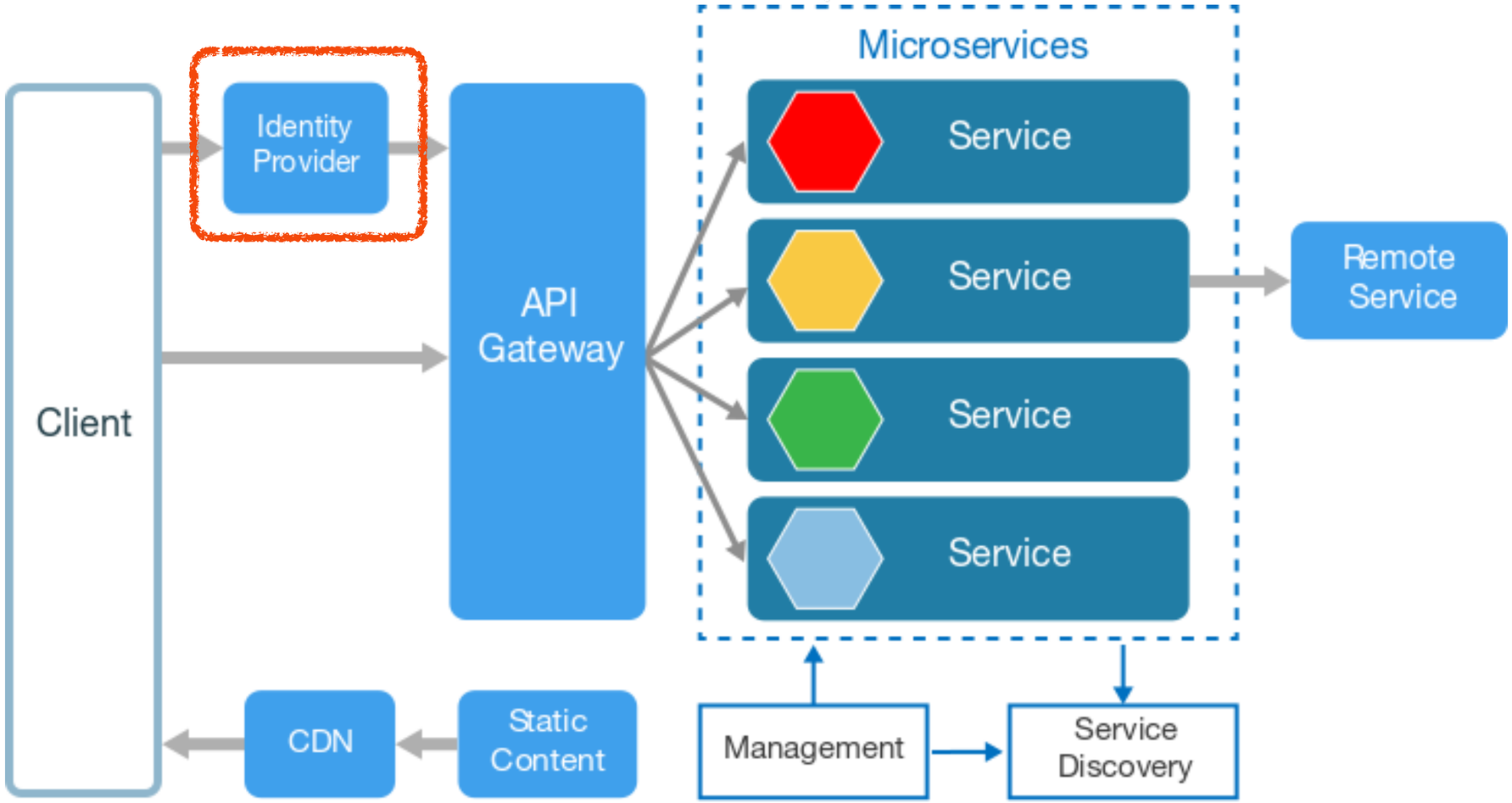


@itrjwyss



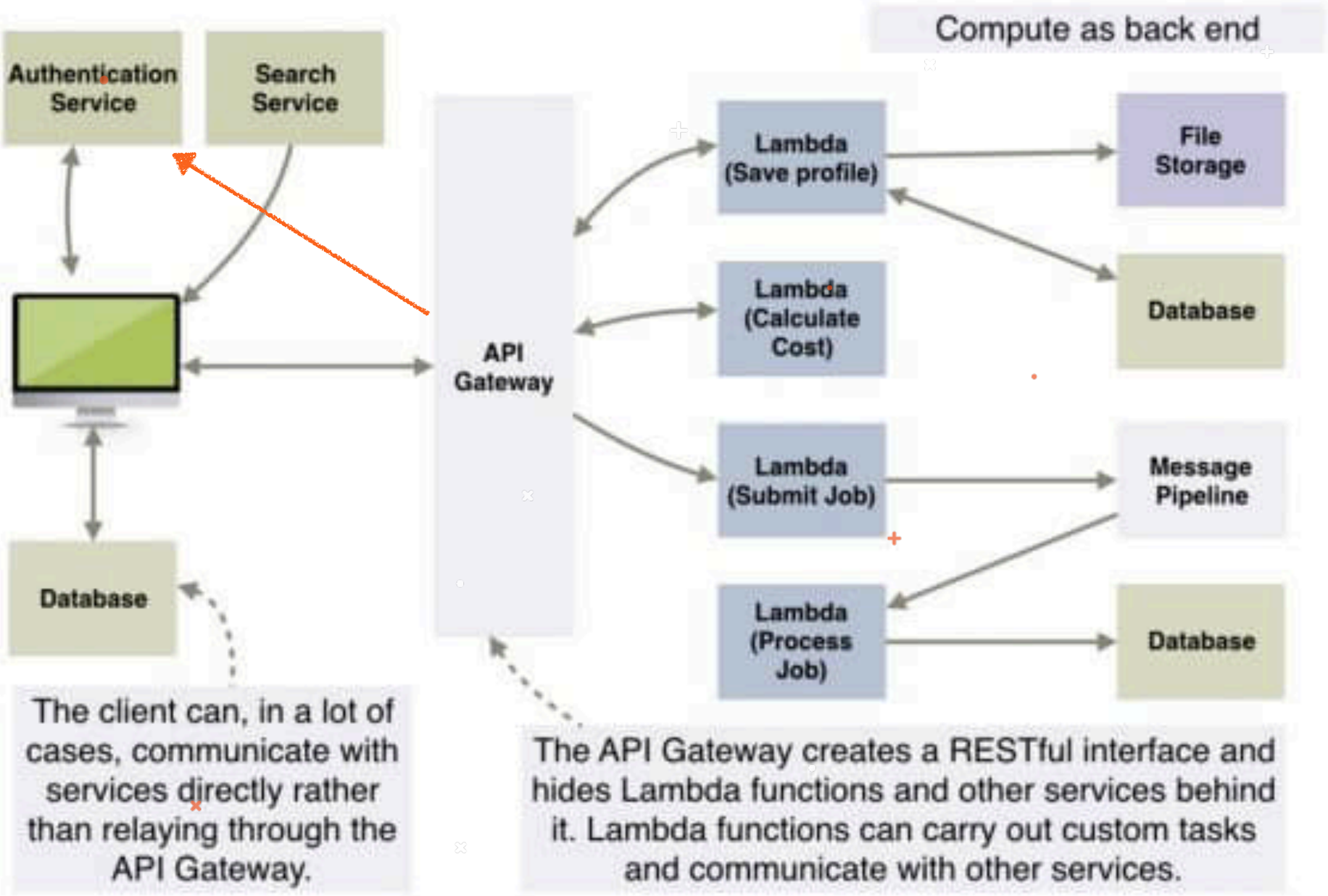
@itrjwyss

Oracle Groundbreaker Ambassador



@itrjwyss

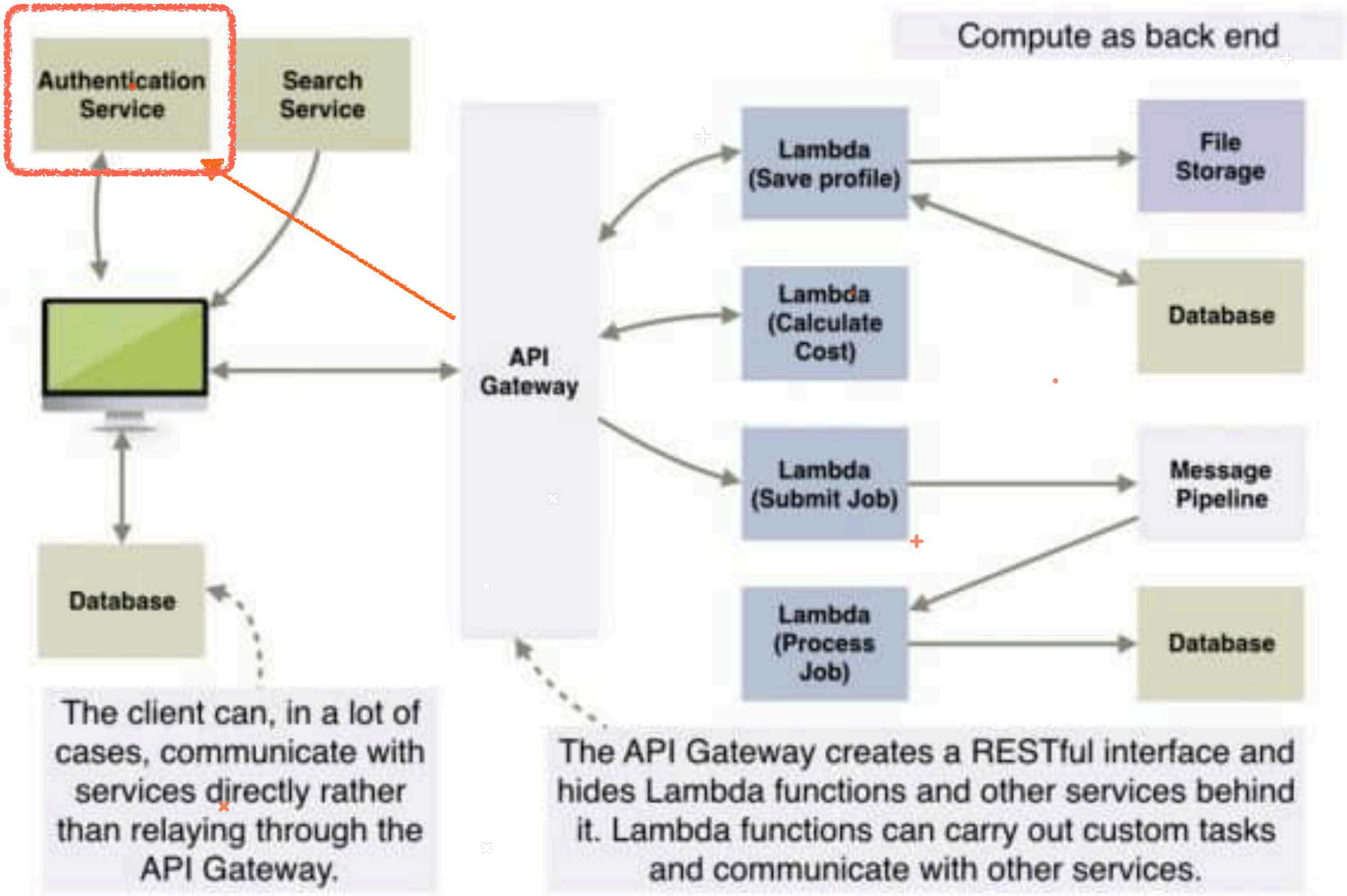
Oracle Groundbreaker Ambassador



@itrjv

Figure 2: The front end can communicate with services directly and invoke Lambda functions through the API Gateway (Sbarski, Serverless Architectures on AWS, 2016).

AMBASSADOR



@itrjv

Figure 2: The front end can communicate with services directly and invoke Lambda functions through the API Gateway (Sbarski, Serverless Architectures on AWS, 2016).

AMBASSADOR

Identity as a Service
IDaaS

@itrjwyss

Oracle
Groundbreaker
Ambassador

IDaaS

- Comprises cloud-based solutions for IdM and IAM functions.
- Also means collecting intelligence to better understand, monitor, and improve their behaviors.

Popular Clouds

Azure Active Directory

ORACLE®

IDENTITY MANAGEMENT

Firebase

Authentication

Auth0

@itrjwyss

Oracle
Groundbreaker
Ambassador

Other Popular IDaaS

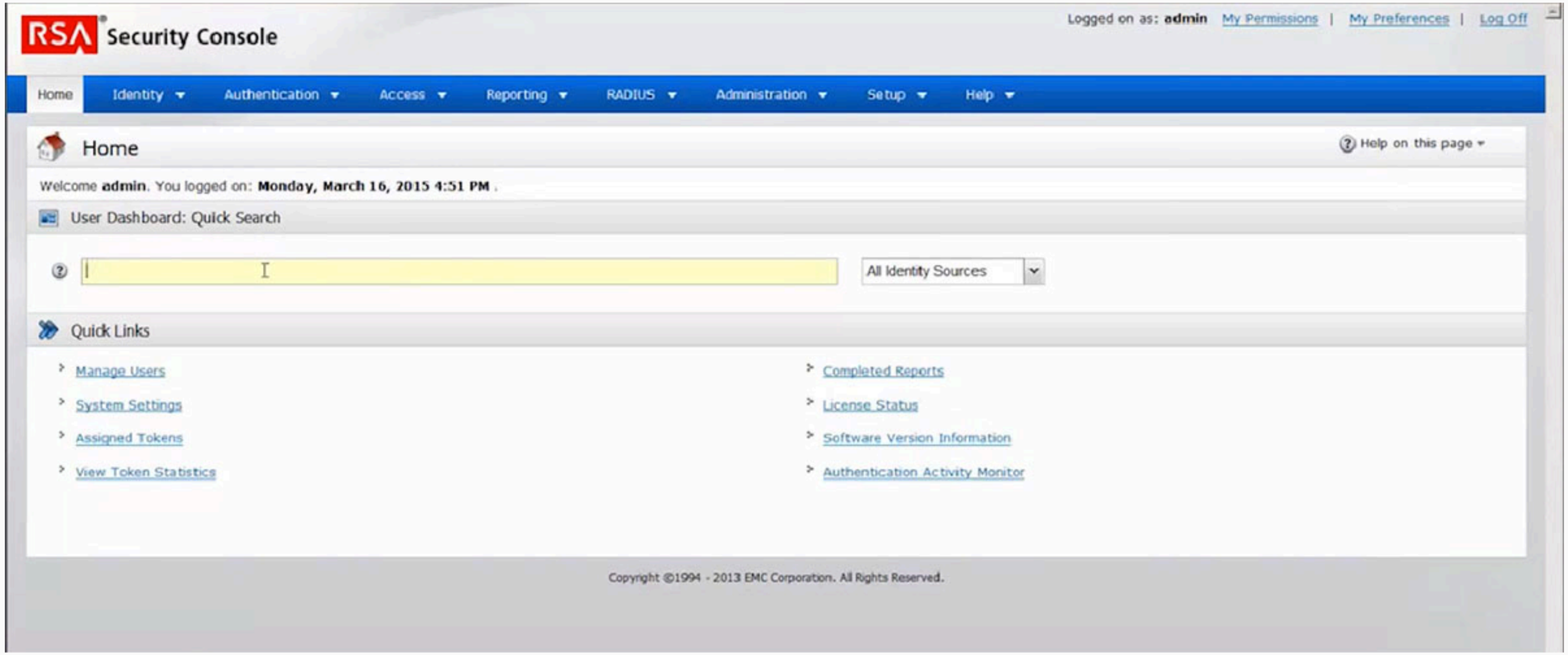
okta

WSO2

@itrjwyss

AMBASSADOR

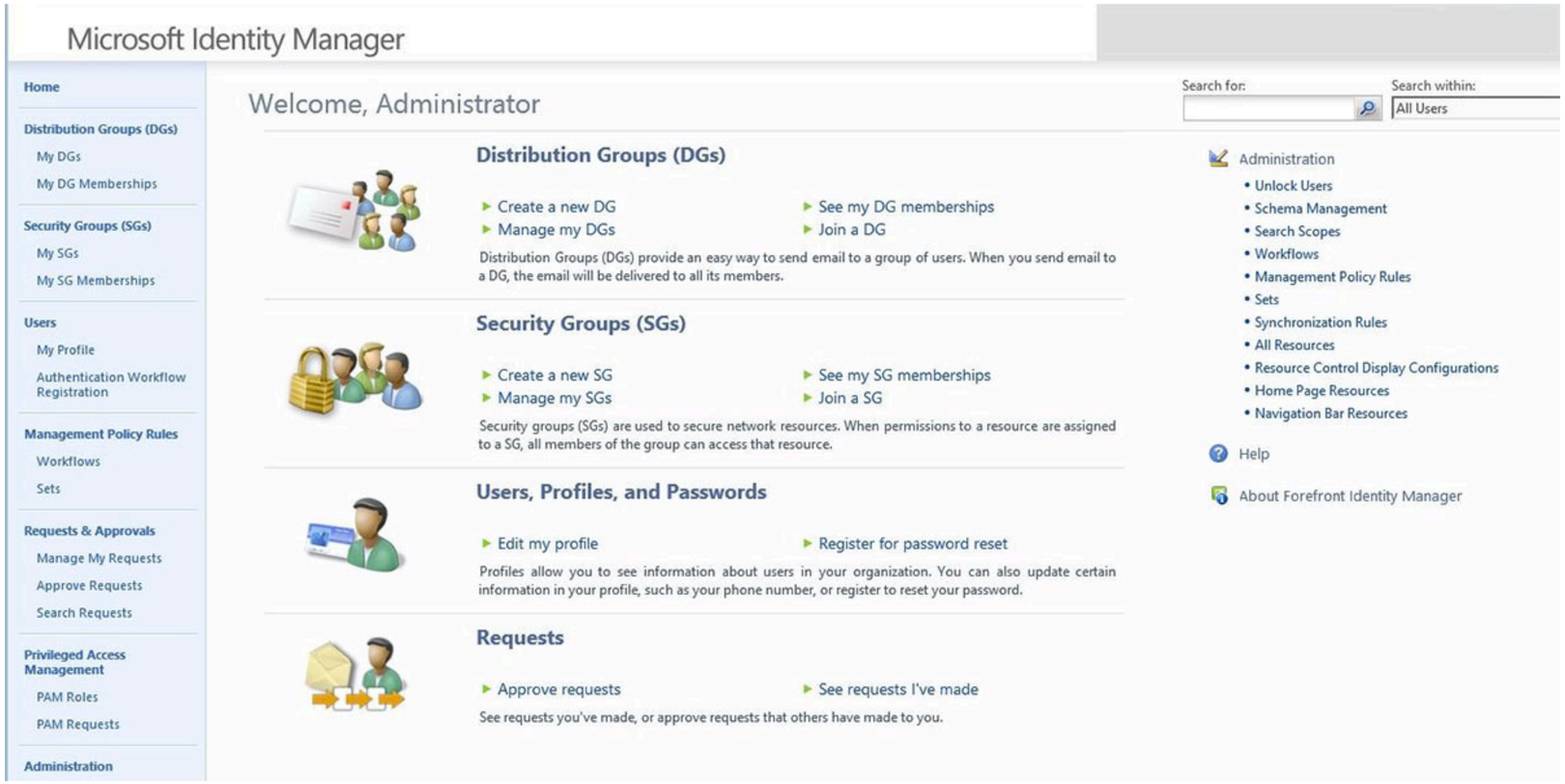
RSA SecurID



@itrjwyss

Oracle Groundbreaker Ambassador

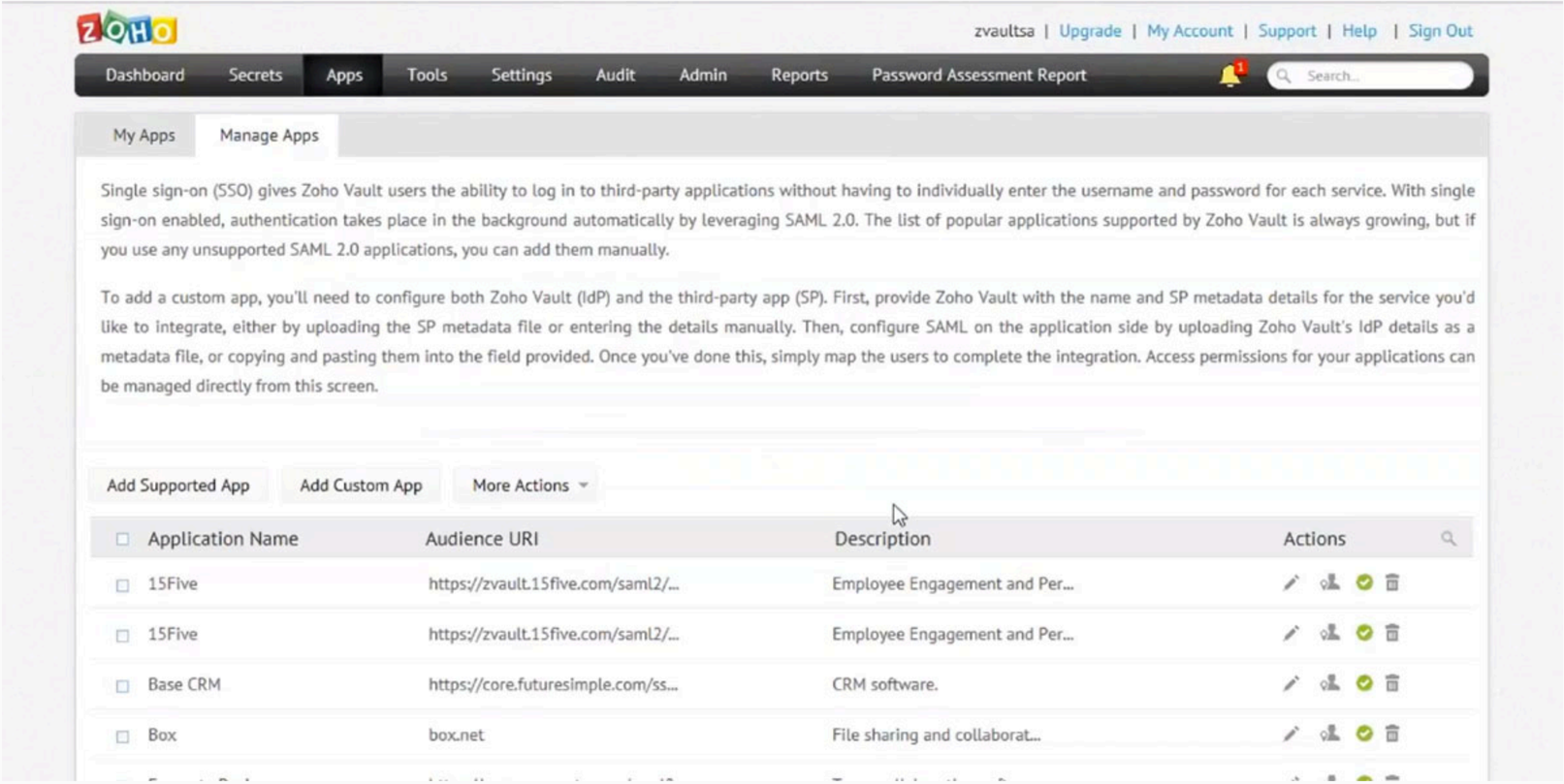
Forefront Identity Manager



@itrjwyss

AMBASSADOR

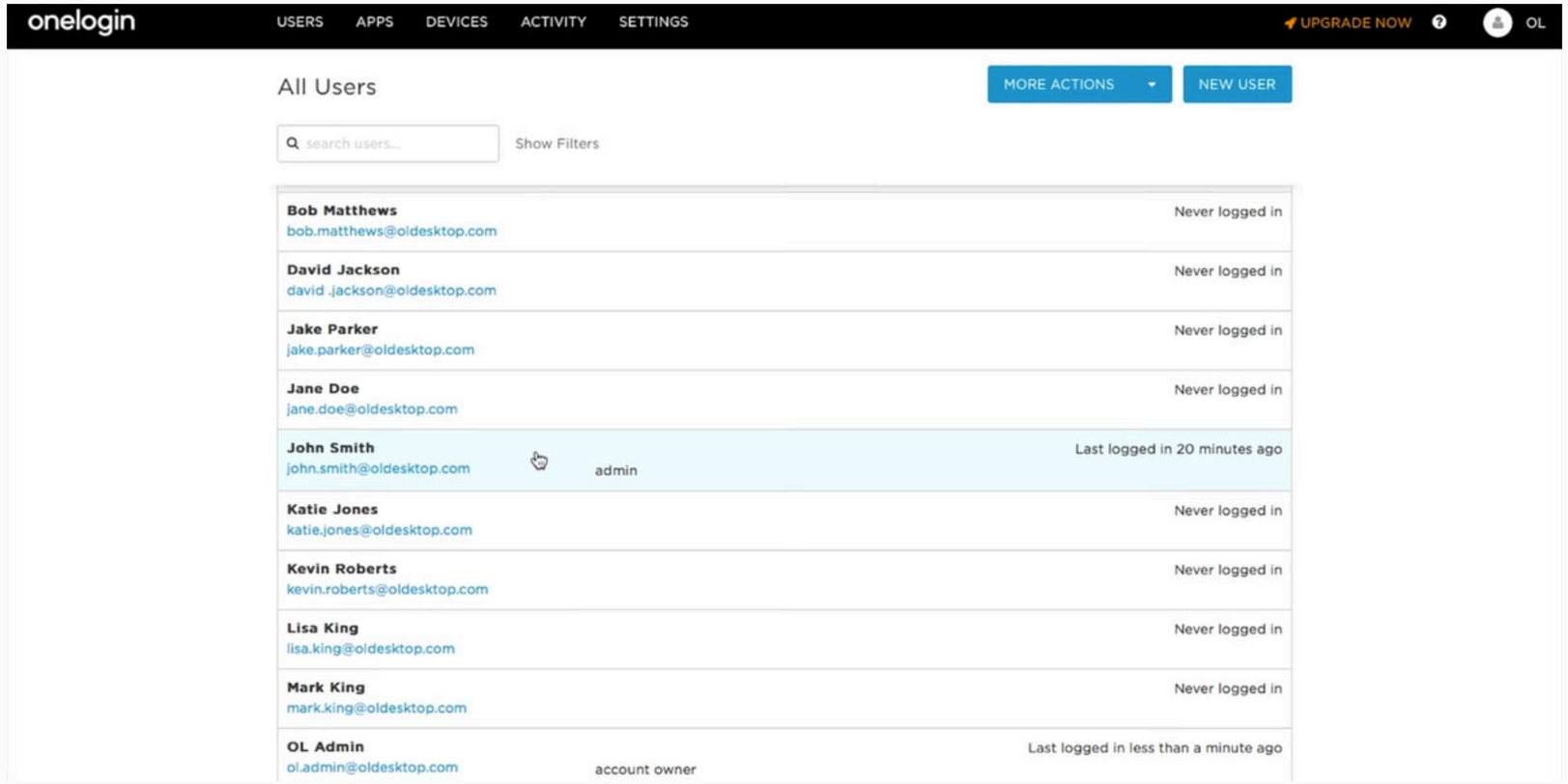
Zoho Vault



@itrjwyss

Oracle Groundbreaker Ambassador

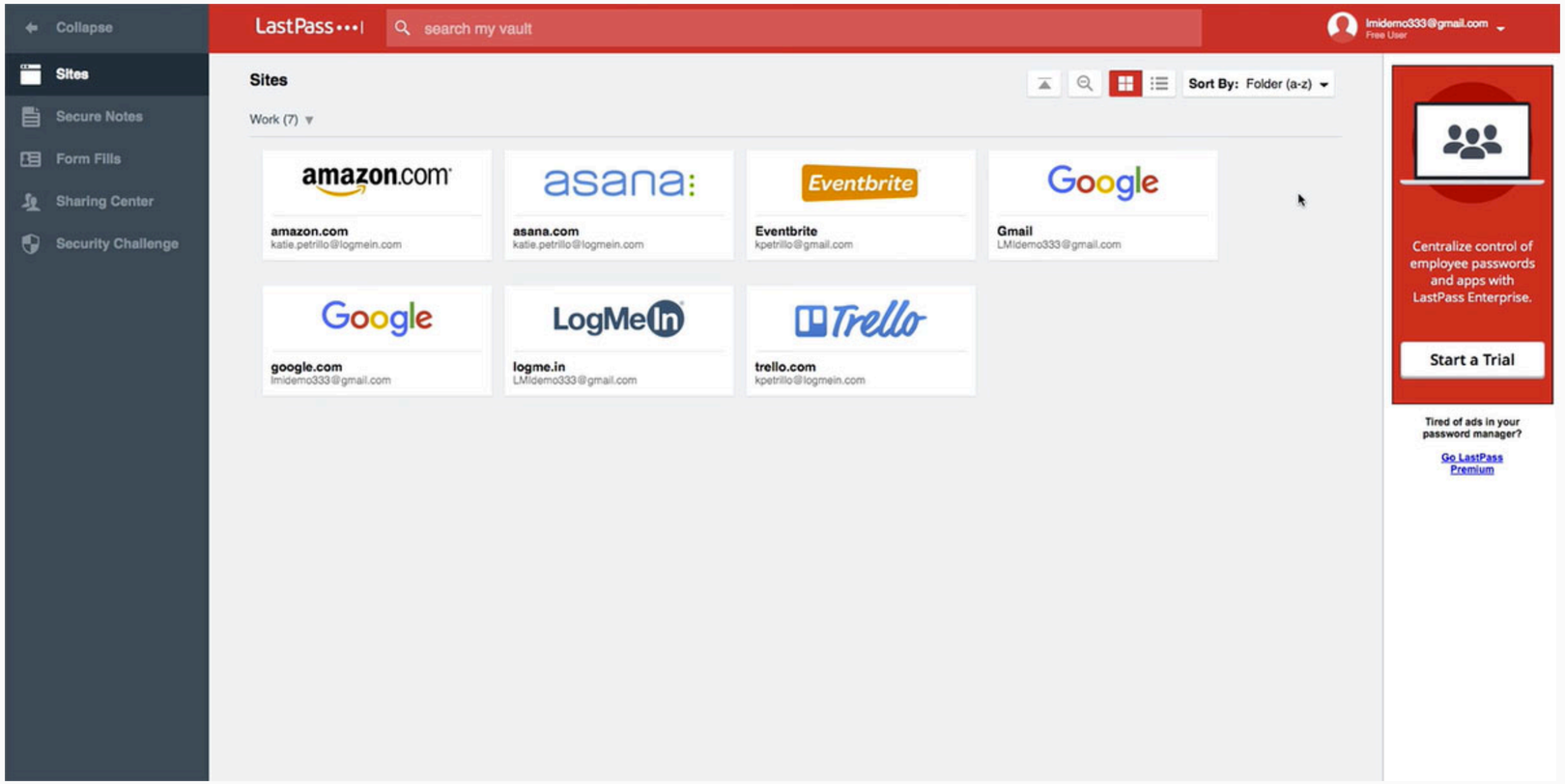
OneLogin



@itrjwyss

AMBASSADOR

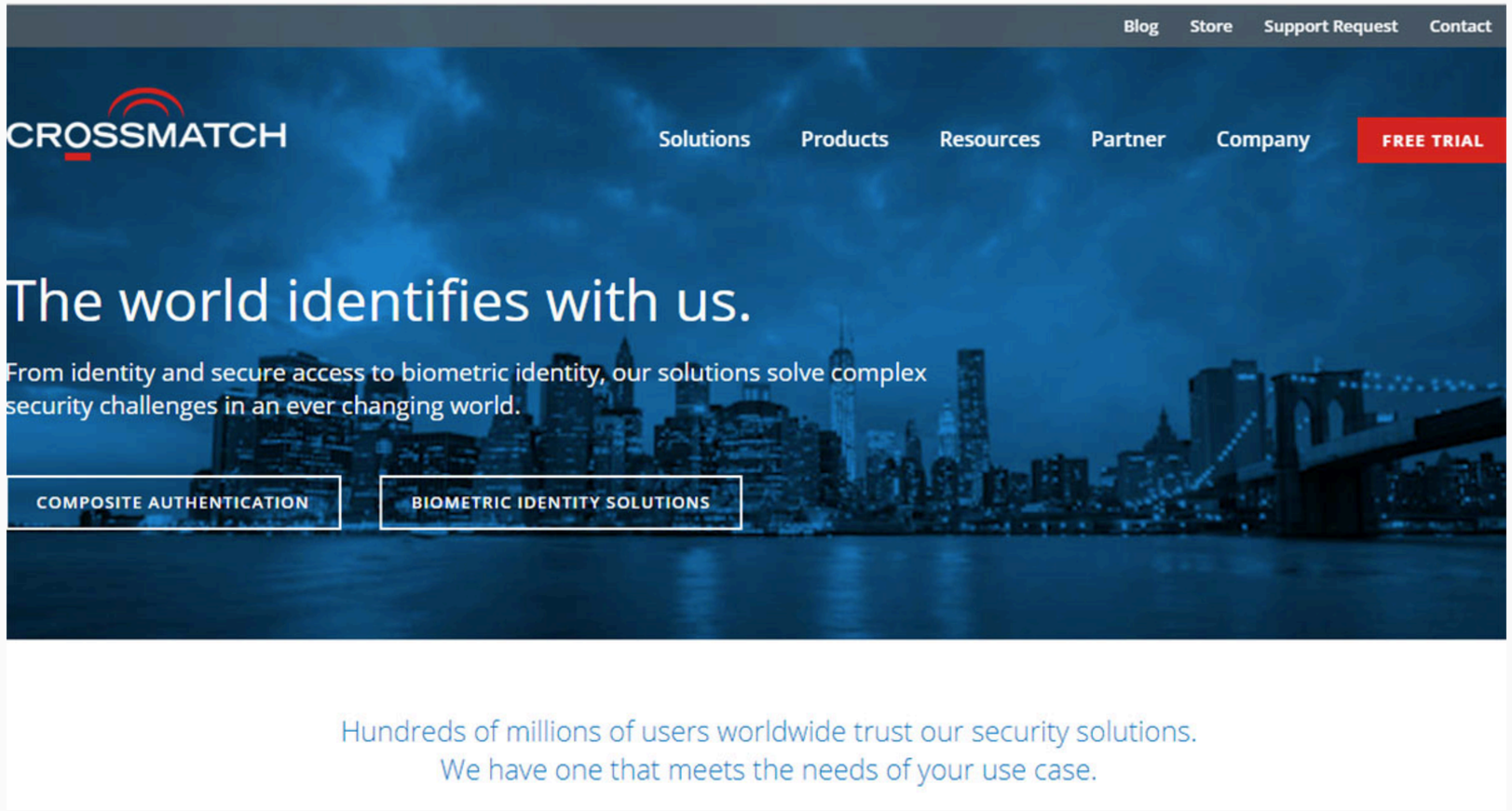
LogMeIn Pro



@itrjwyss

Oracle Groundbreaker Ambassador

Digital Persona



@itrjwyss

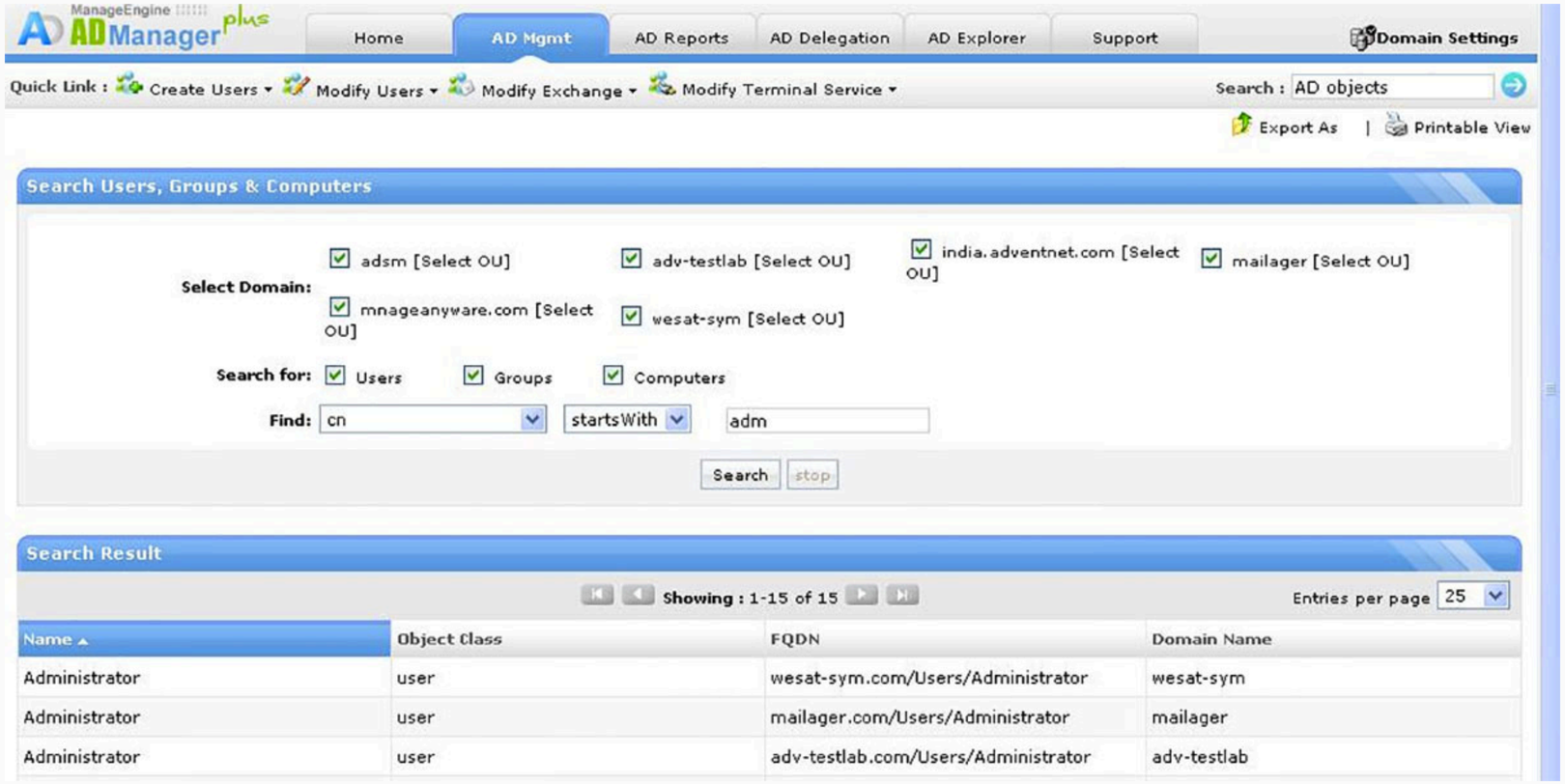
AMBASSADOR

ExcelID

@itrjwyss

Oracle Groundbreaker Ambassador

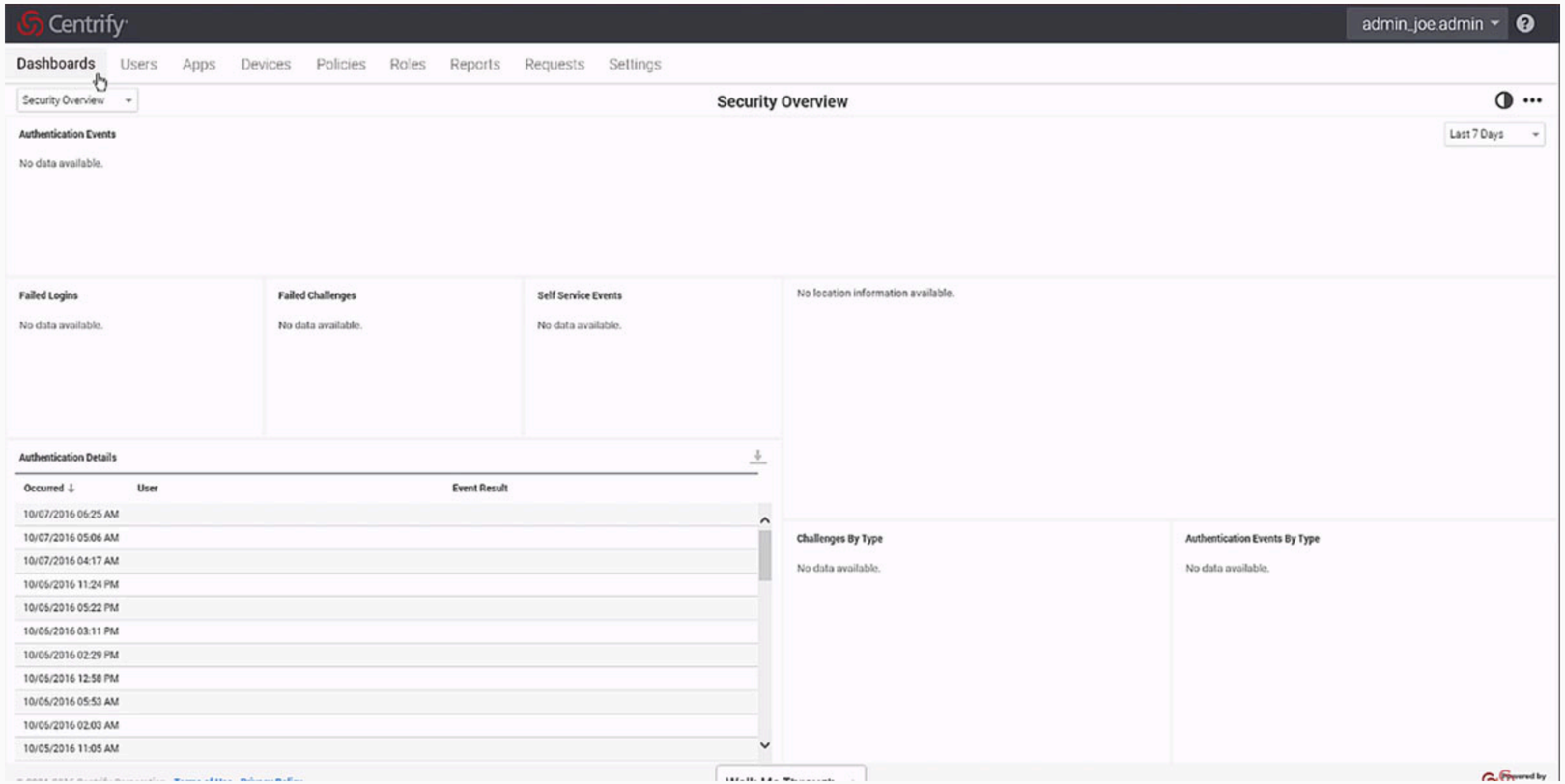
ADManager Plus



@itrjwyss

AMBASSADOR

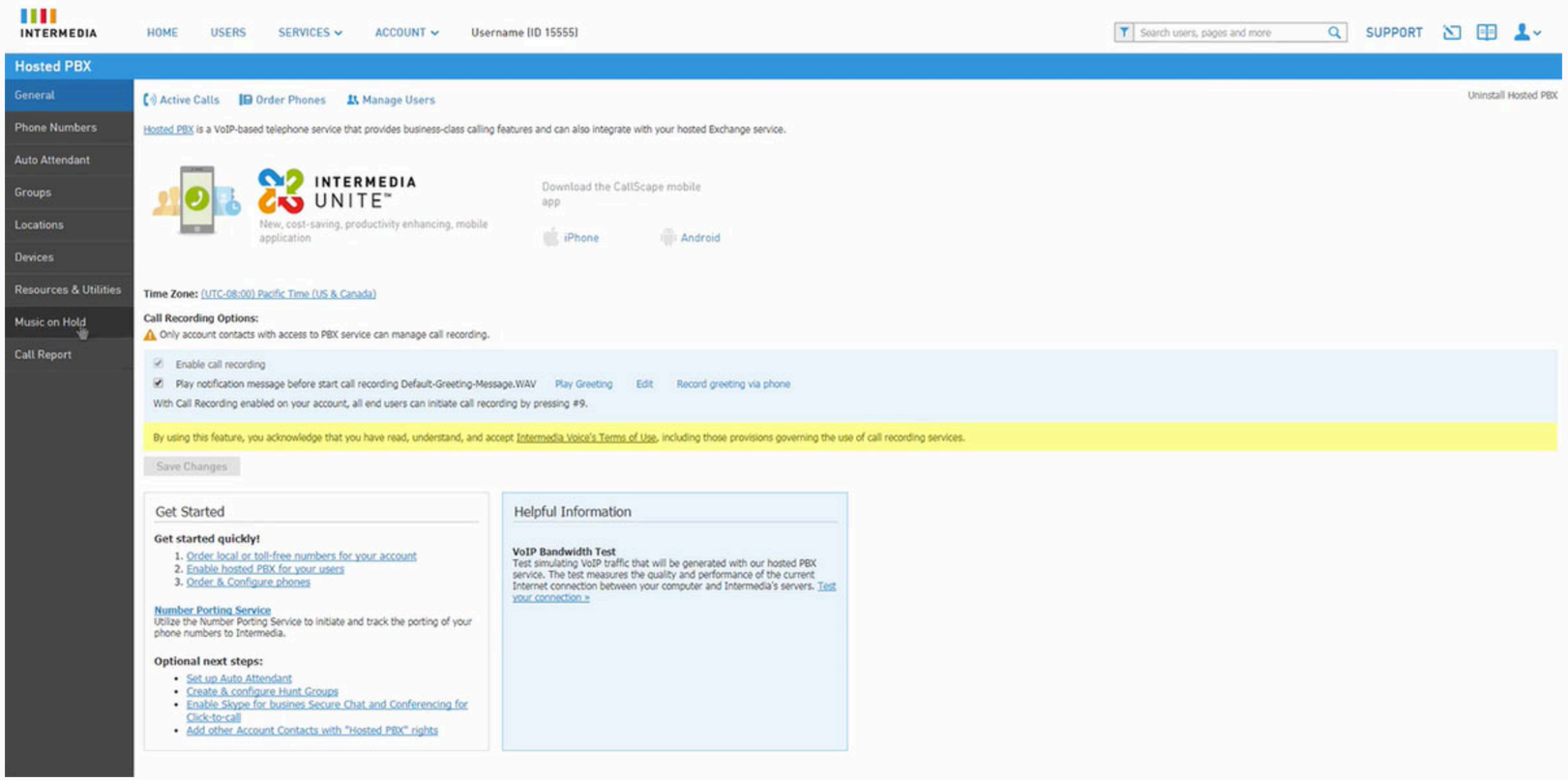
Centrify Identity Service



@itrjwyss

Oracle Groundbreaker Ambassador

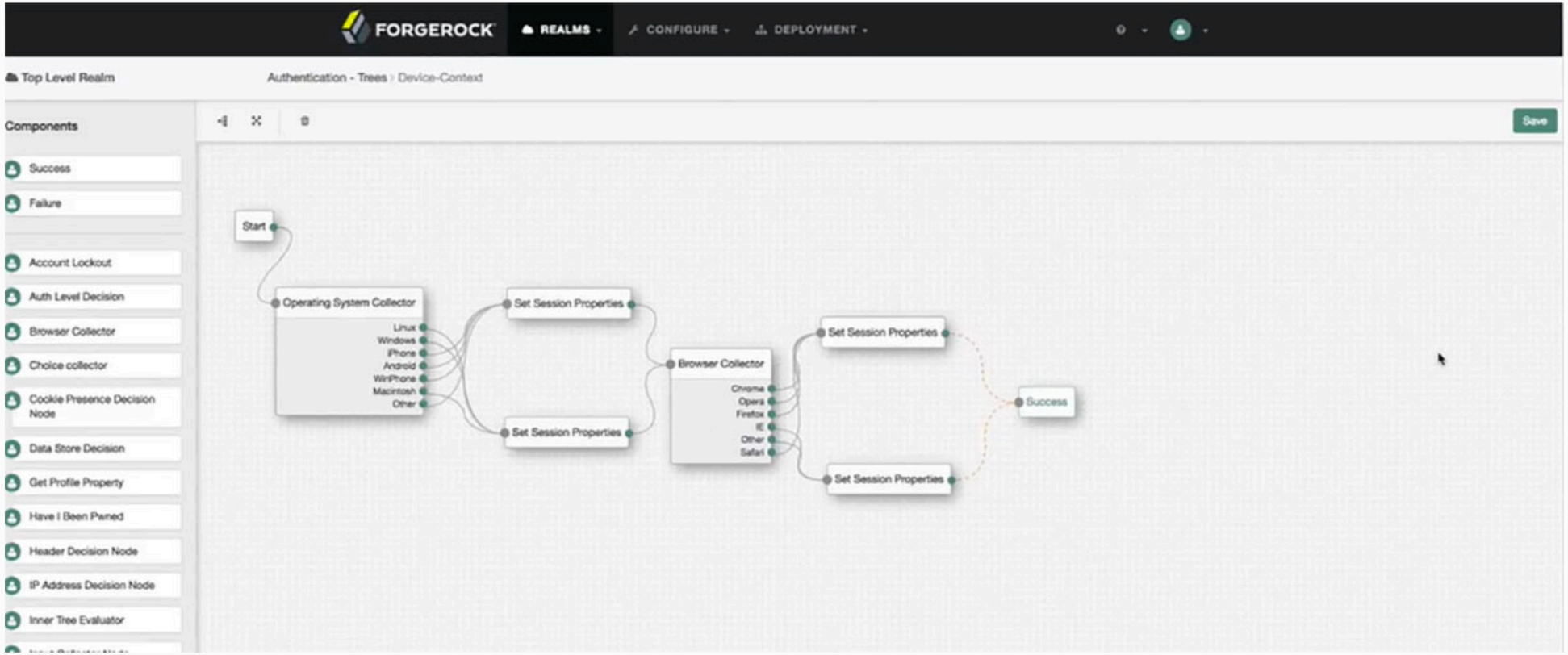
Intermedia AppID Enterprise



@itrjwyss

AMBASSADOR

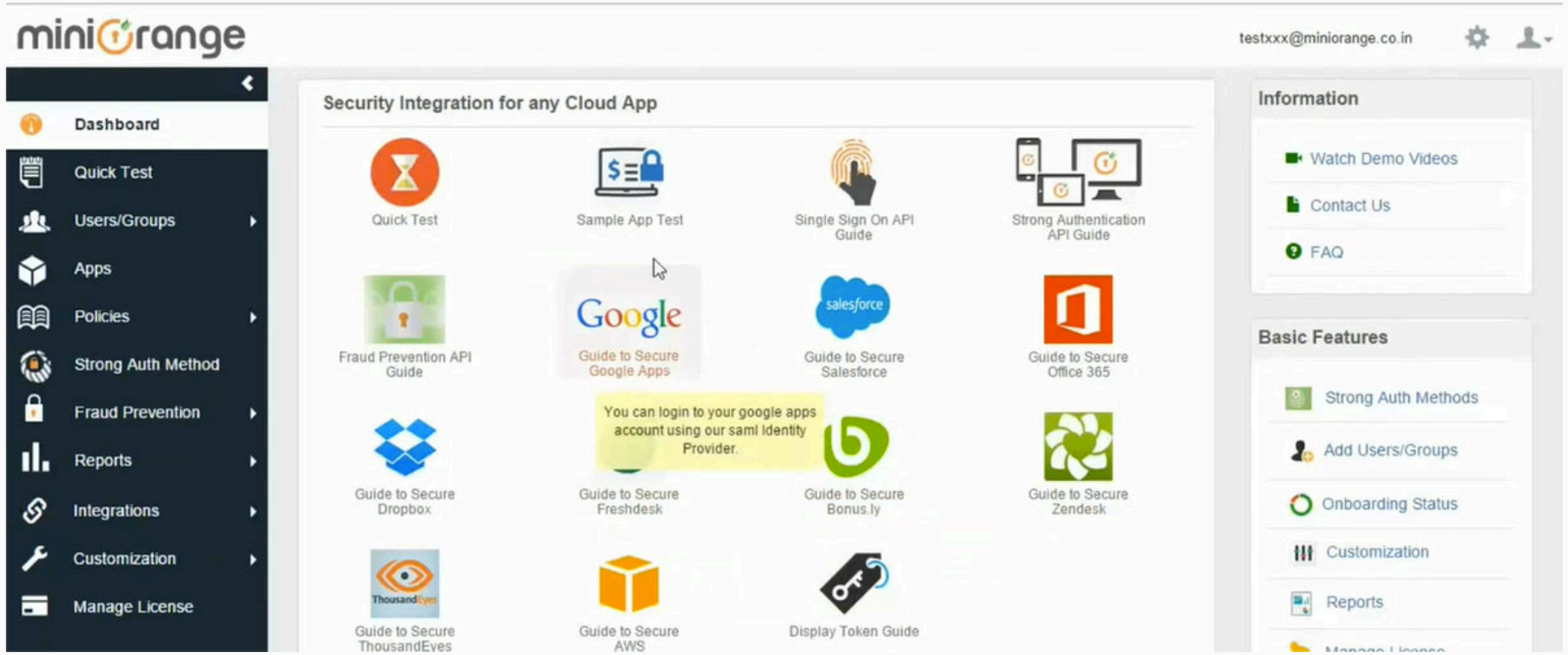
ForgeRock Identity Platform



@itrjwyss

Oracle Groundbreaker Ambassador

MiniOrange



@itrjwyss

AMBASSADOR

NetIQ IDM

NetIQ.

- Planning to Install the Remote Loader
- Installing Remote Loader
  - Using the Wizard to Install the Remote Loader
  - Performing a Silent Installation of the Remote Loader
  - Installing Java Remote Loader
- Configuring the Remote Loader and Drivers
  - Creating a Secure Connection to the Identity Manager Engine
  - Understanding the Configuration Parameters for the Remote Loader
  - Configuring the Remote Loader for Driver Instances on UNIX or Linux
  - Configuring the Remote Loader for Driver Instances on Windows
  - Configuring the Java Remote Loader for Driver Instances
  - Configuring Identity Manager Drivers to Work with the Remote Loader
  - Verifying the Configuration
- Starting and Stopping the Remote Loader
- Installing iManager
- Installing Designer for Identity Manager

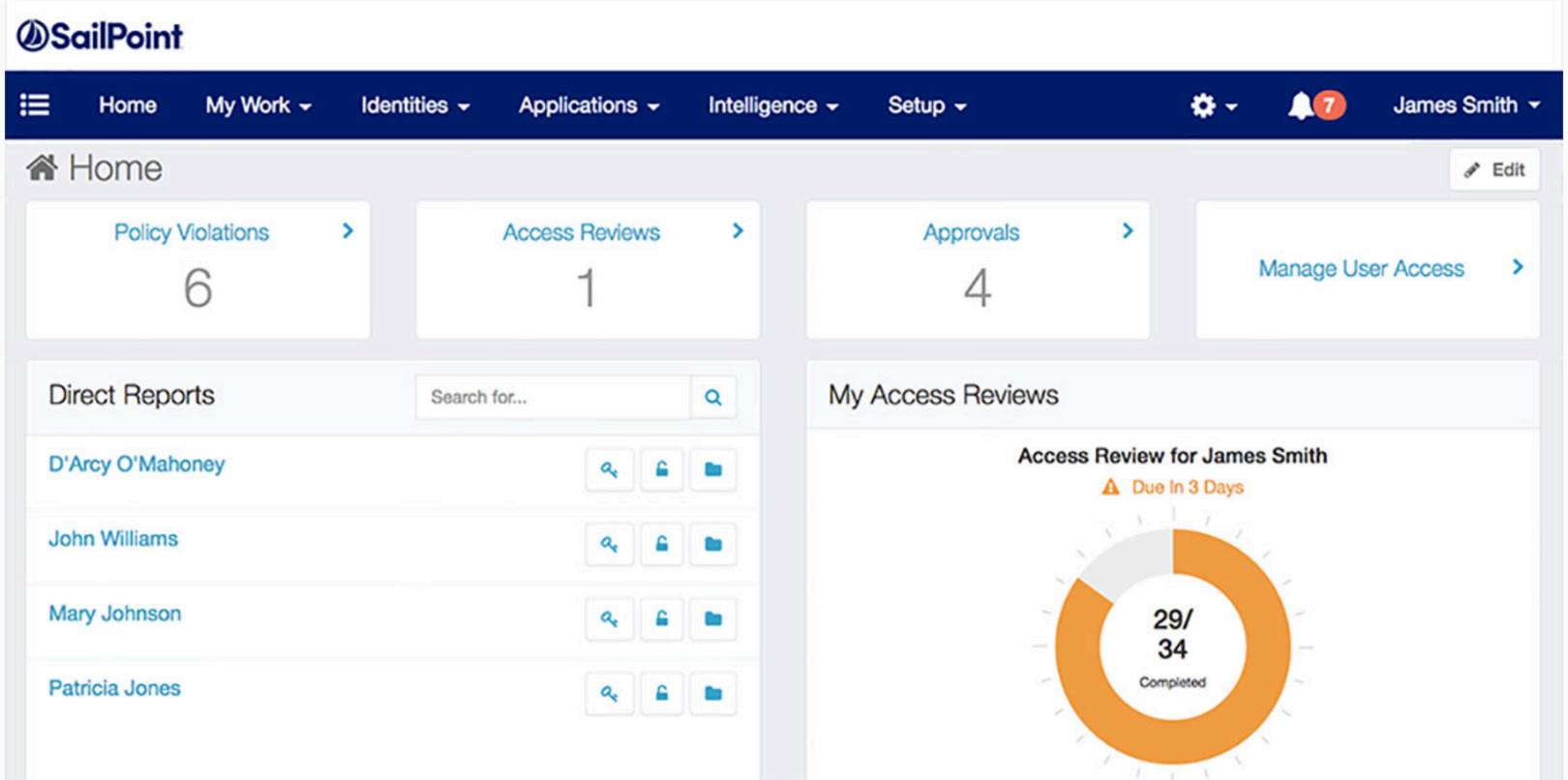
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback Driver
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Oracle User Management Driver
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Oracle HR Driver
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Oracle TCA Driver
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	Managed System Gateway Driver
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Manual Task Driver
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS Driver
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes Driver
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft Driver
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Privileged User Management Driver
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	Salesforce Driver
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	SAP Portal Driver
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	SAP User Management Driver
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP Driver
com.novell.idm.driver.ComposerDriverShim	User Application
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder Driver

comment on this topic

@itrjwyss

Oracle Groundbreaker Ambassador

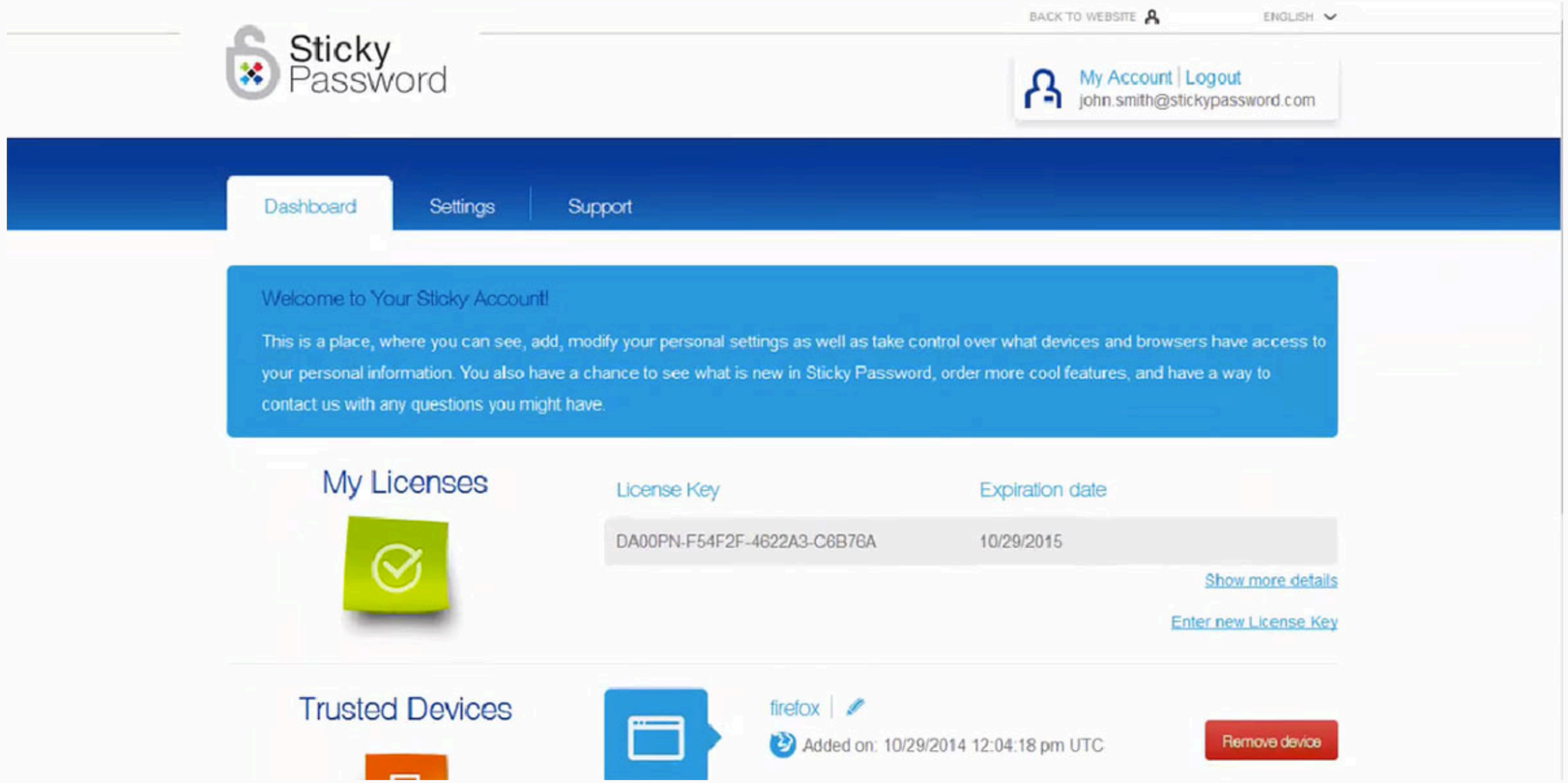
Sail Point



@itrjwyss

AMBASSADOR

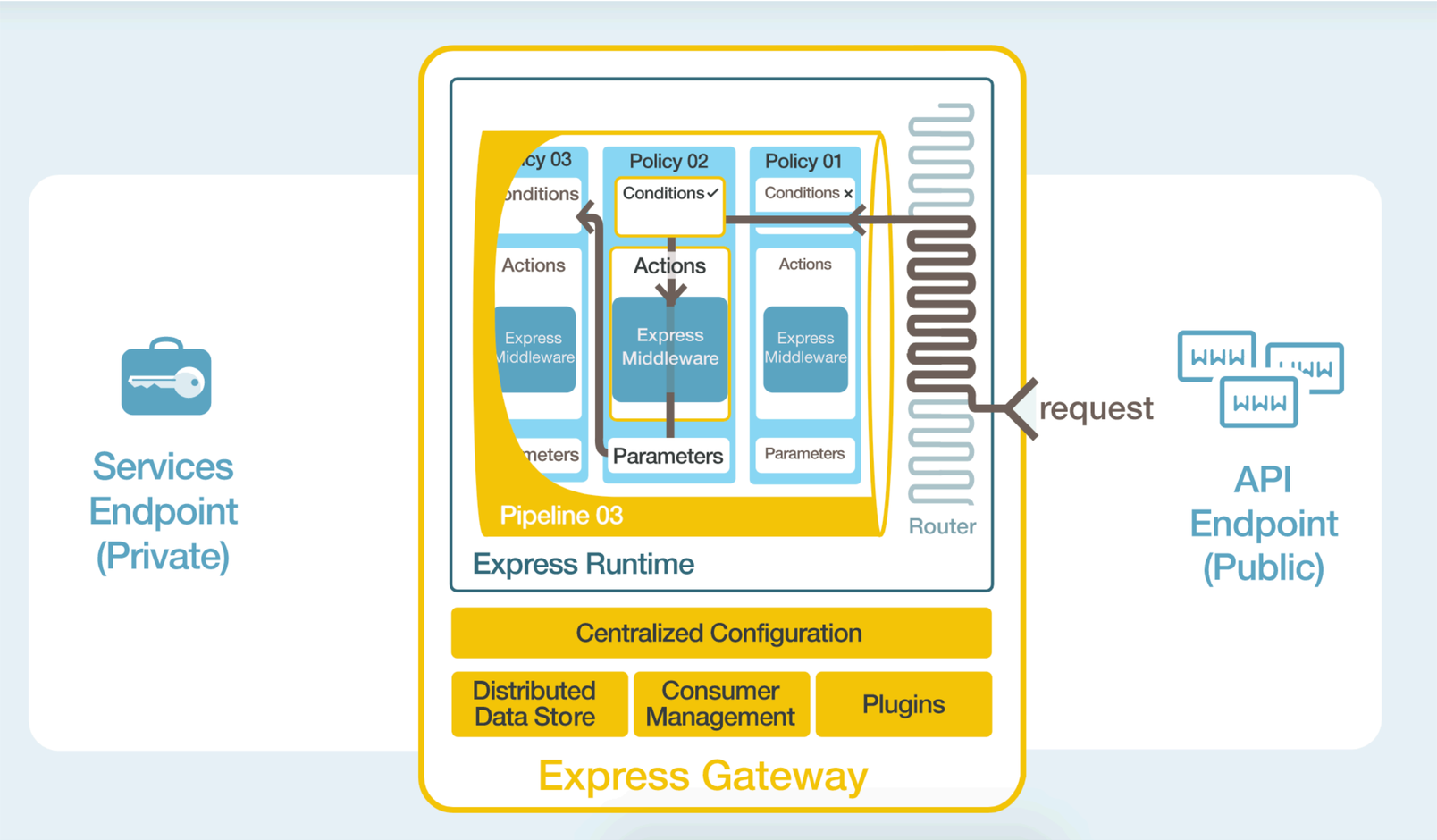
Sticky Password



@itrjwyss

Oracle Groundbreaker Ambassador

Express Gateway



@itrjwyss

Scenarios

Customers
http://customers

Order
http://orders

Express Gateway

```
$ npm i -g express-gateway

+ express-gateway@1.15.0
added 596 packages from 402 contributors in 105.983s

$ eg gateway create
? What's the name of your Express Gateway? eg-example
? Where would you like to install your Express Gateway? eg-example
? What type of Express Gateway do you want to create? Getting Started with Express Gateway
   create package.json
   create server.js
   create config/gateway.config.yml
   create config/system.config.yml
   create config/models/applications.json
   create config/models/credentials.json
   create config/models/users.json

...

To start eg-example, run the following commands:
    cd eg-example && npm start
```

@itrjwyss

gateway.config.yml

```yaml
http:
  port: 80
apiEndpoints:
  customers:
    host: customer.company.com
  orders:
    host: orders.company.com
  other:
    host: localhost
serviceEndpoints:
  customers:
    url: 'http://customers'
  orders:
    url: 'http://orders'
policies:
  - jwt
  - proxy
  - rate-limit
```

@itrjwyss

Oracle Groundbreaker Ambassador

gateway.config.yml

```yaml
pipelines:
  customers:
    apiEndpoints:
      - customers
    policies:
      - rate-limit:
          - action:
              max: 1
              windowMs: 1000
      - jwt:
          - action:
              secretOrPublicKeyFile: ./key/pubKey.pem
              checkCredentialExistence: false
      - proxy:
          - action:
              serviceEndpoint: customers
              changeOrigin: true
```

@itrjwyss

AMBASSADOR

gateway.config.yml

```yaml
pipelines:
  orders:
    apiEndpoints:
      - orders
    policies:
      - rate-limit:
          - action:
              max: 1
              windowMs: 1000
      - jwt:
          - action:
              secretOrPublicKeyFile: ./key/pubKey.pem
              checkCredentialExistence: false
      - proxy:
          - action:
              serviceEndpoint: customers
              changeOrigin: true
```

@itrjwyss

Oracle Groundbreaker Ambassador

Testing

```
$ curl http://customers.company.com:8080 & curl http://customers.company.com:8080
$ [1] 4495
$ Unauthorized
$ [1]+  Done
$ Too many requests, please try again later.
```

@itrjwyss

Testing

```
export JWT=“ey...the-rest-of-the-token"
curl -H "Authorization: Bearer "$JWT http://customers.company.com:8080
```

https://github.com/itrjwyss/ModernIdM/

https://www.facebook.com/itrjwyss

@itrjwyss

AMBASSADOR