Modern Identity Management

in the era of Serverless and Microservices

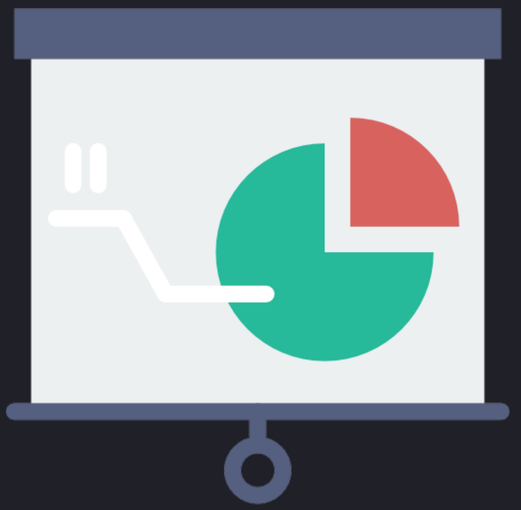
VERSION 2.0


Security
Matters
AMBASSADOR

US Data Breaches Statistics

54%
Increase in the first half of 2019

3,800+
were reported



3.2 billion
Just 8 of those


EQUIFAX
AMBASSADOR

Had Been Uploaded

38,000
Driver's Licenses

3,200
Passport Details

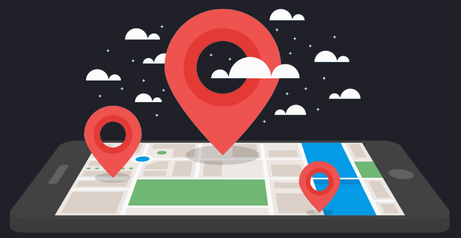
@itrjwyss

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

AMBASSADOR

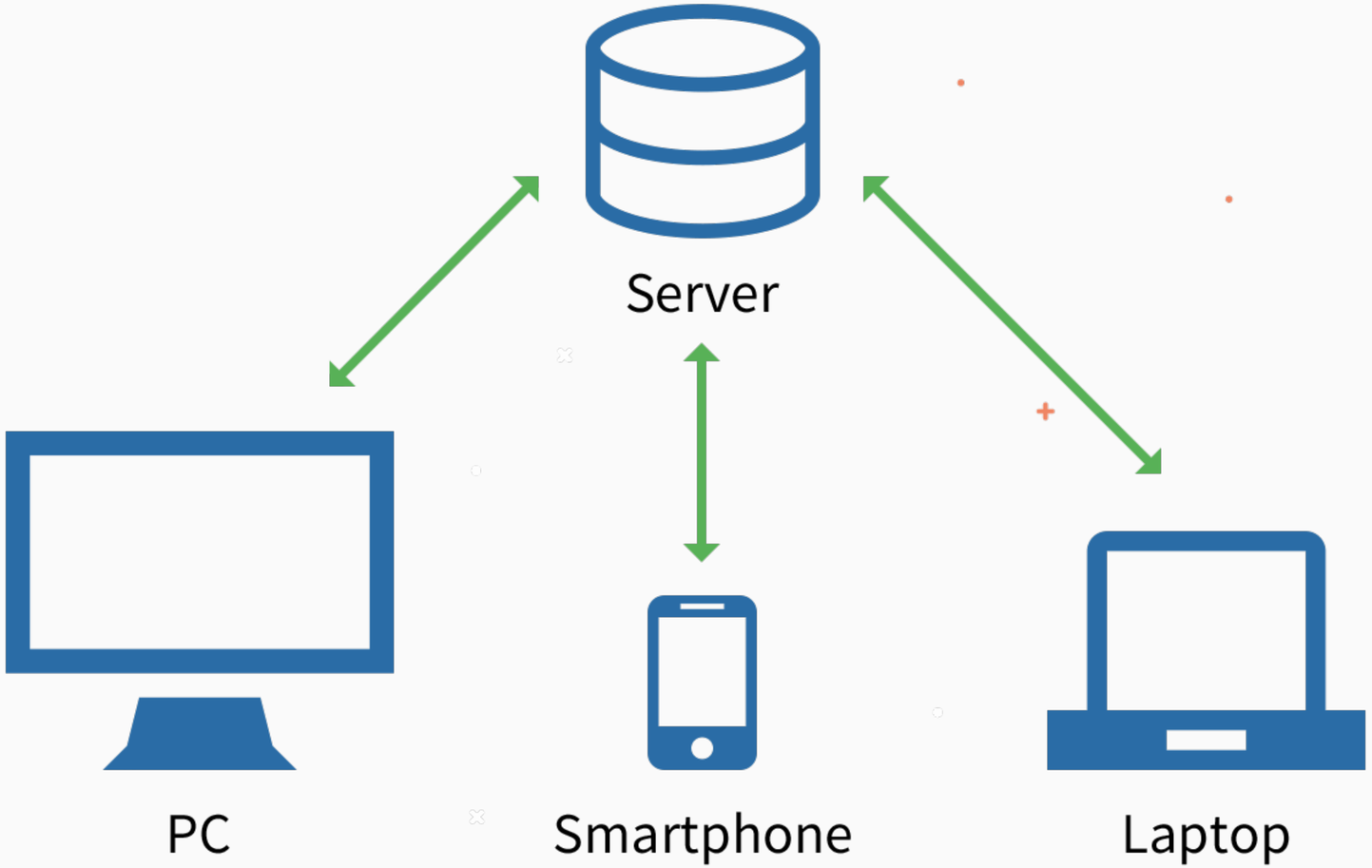
EU General Data Protection Regulation

25 May 2018

Oracle Groundbreaker Ambassador


Security must be a goal.
@itrjwyss
AMBASSADOR

Security is a **Team Effort**



Best Practices

Identity Security

@itrjwyss

Talk Roadmap

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

@itrjwyss

Oracle Groundbreaker Ambassador

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

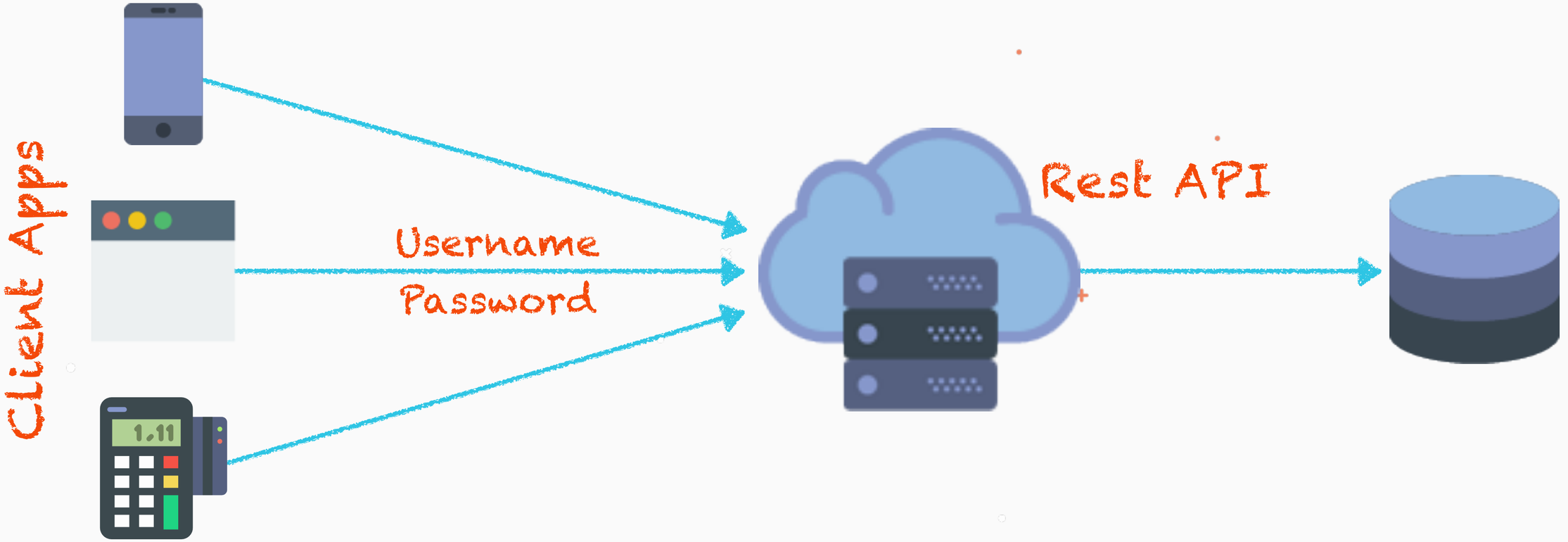
Comunidad Desarrolladores en Tecnologías

< Google > en Guatemala

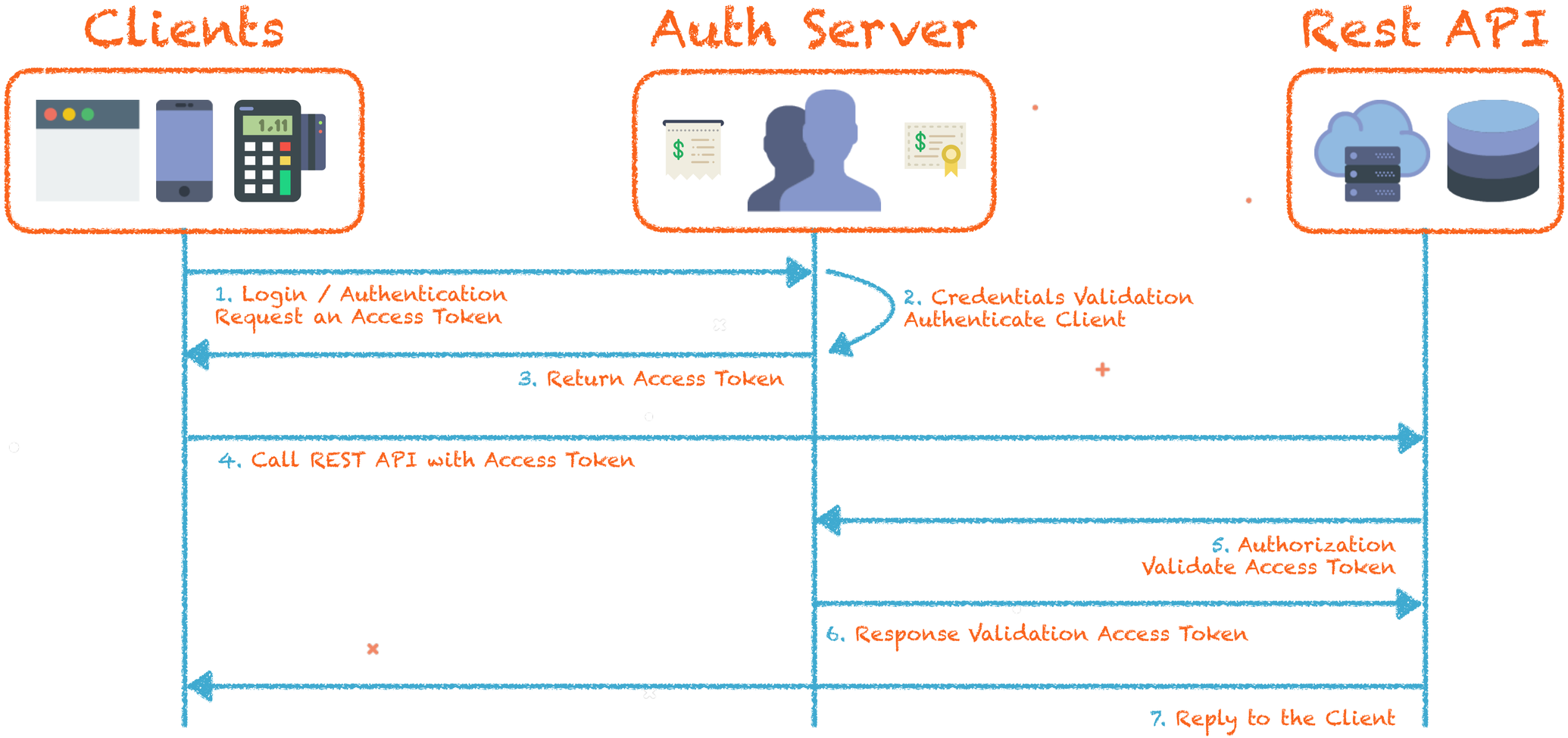
JDuchess

Guatemala

Bad API Design



OAuth



@itrjwyss

AMBASSADOR

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.

Header

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.

Claims

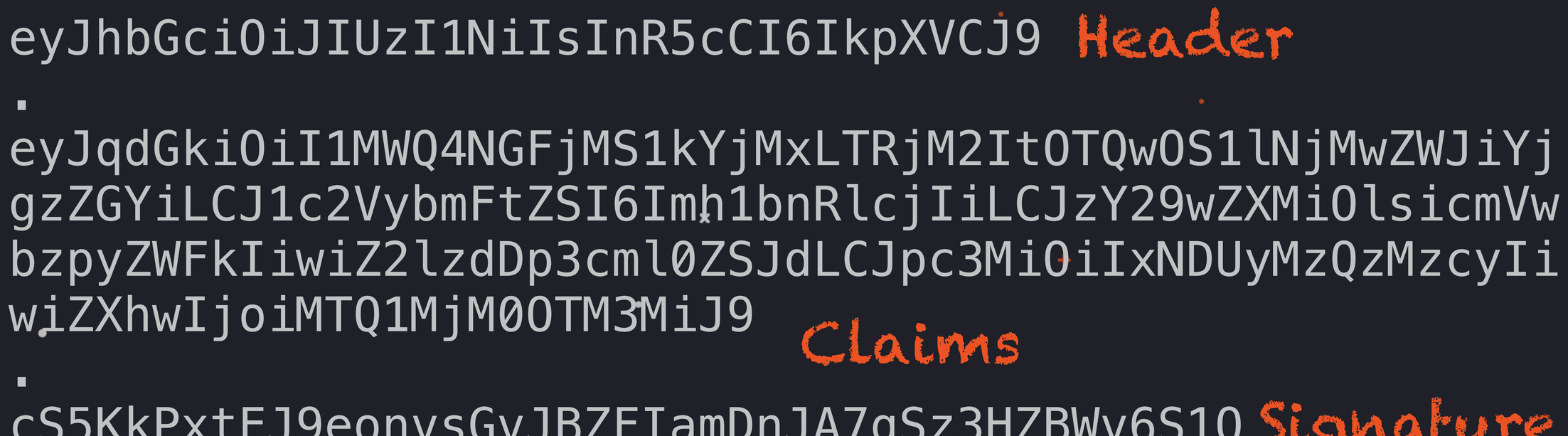
JSON Web Signature
JWT + JWS

@itrjwyss

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



@itrjwyss

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

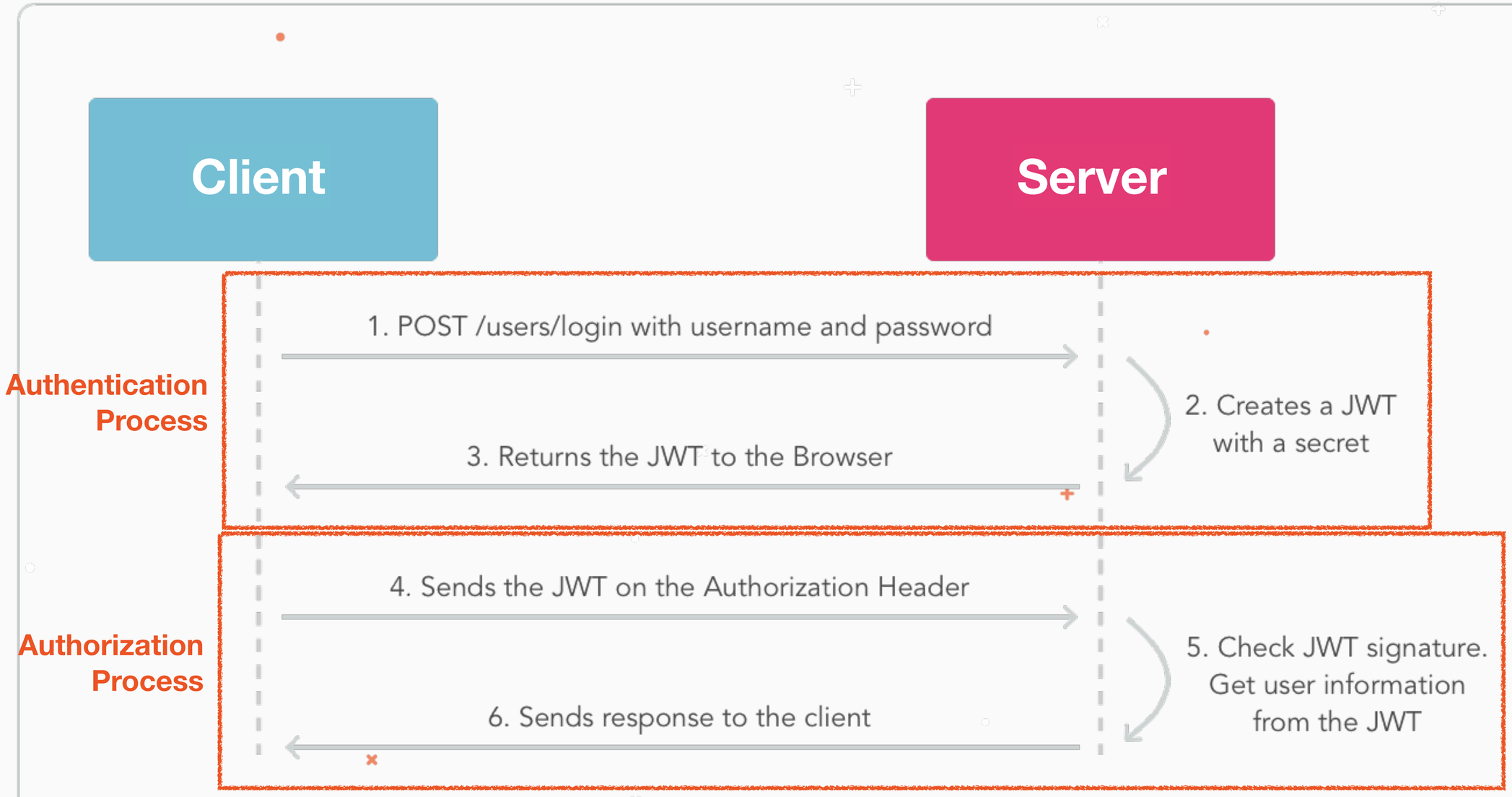
Oracle Groundbreaker Ambassador

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

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

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.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```

Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

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

Oracle Groundbreaker Ambassador

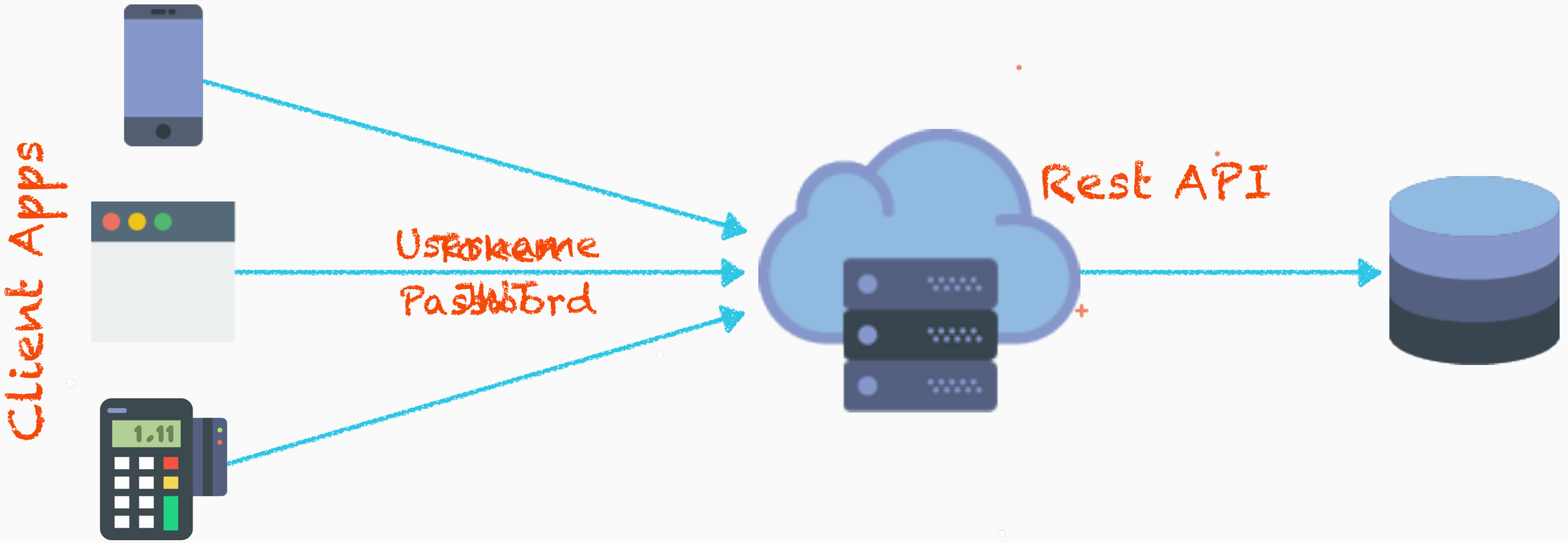
Learn everything you wanted to know, but were afraid to ask about JSON Web Tokens

auth0.com/e-books/jwt-handbook

@itrjwyss

AMBASSADOR

Improve API Design



User Credentials Problem

@itrjwyss

AMBASSADOR

SSO

Single Sign On

@itrjwyss

Oracle Groundbreaker Ambassador


PASSWORD
AMBASSADOR

@itrjwyss

Oracle
Groundbreaker
Ambassador

@itrjwyss

AMBASSADOR

Sorry, but your password must contain an uppercase letter, a number, a hieroglyph, a feather from a hawk and the blood of a unicorn.

Oracle Groundbreaker Ambassador


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

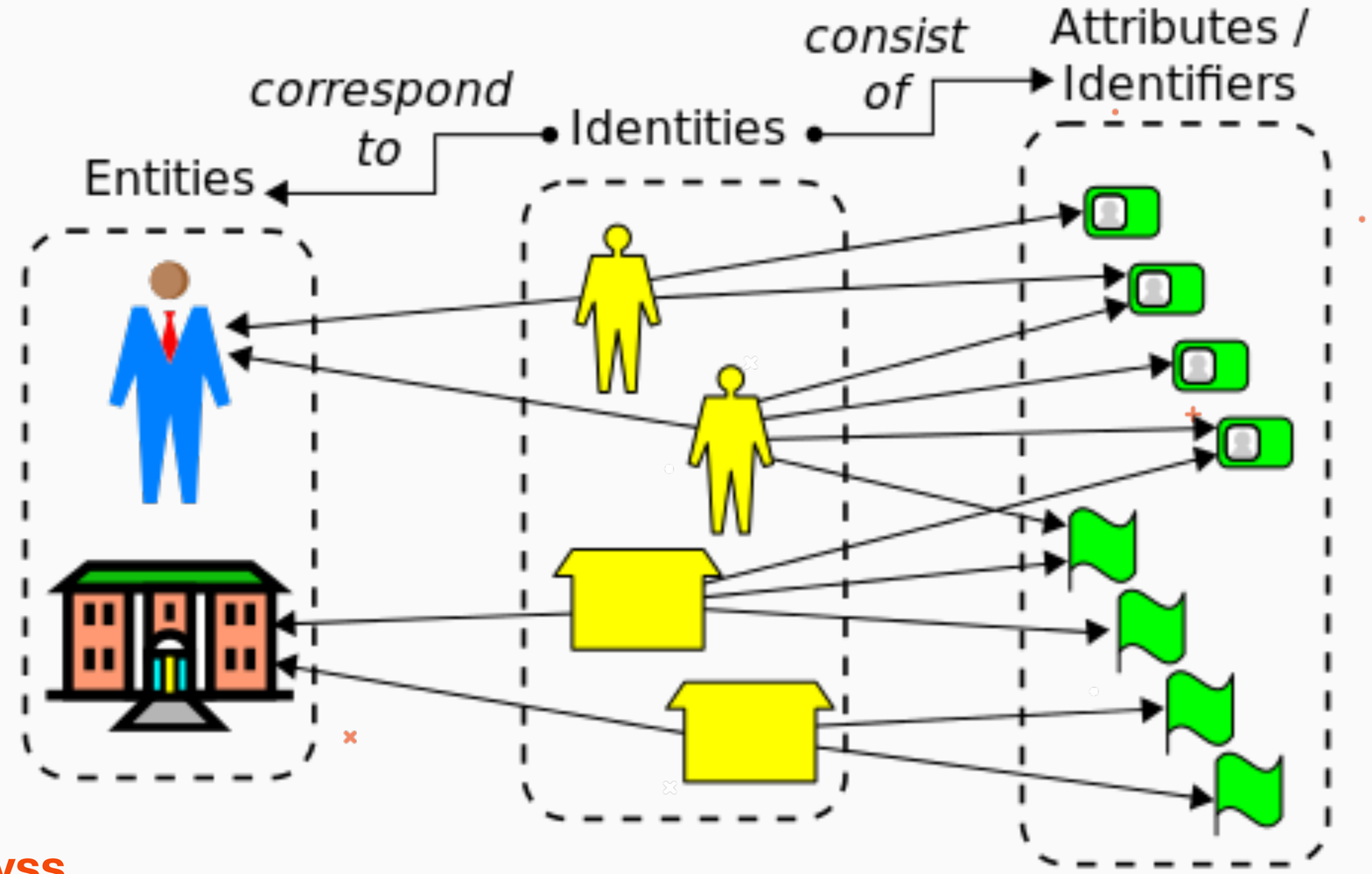
AMBASSADOR

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

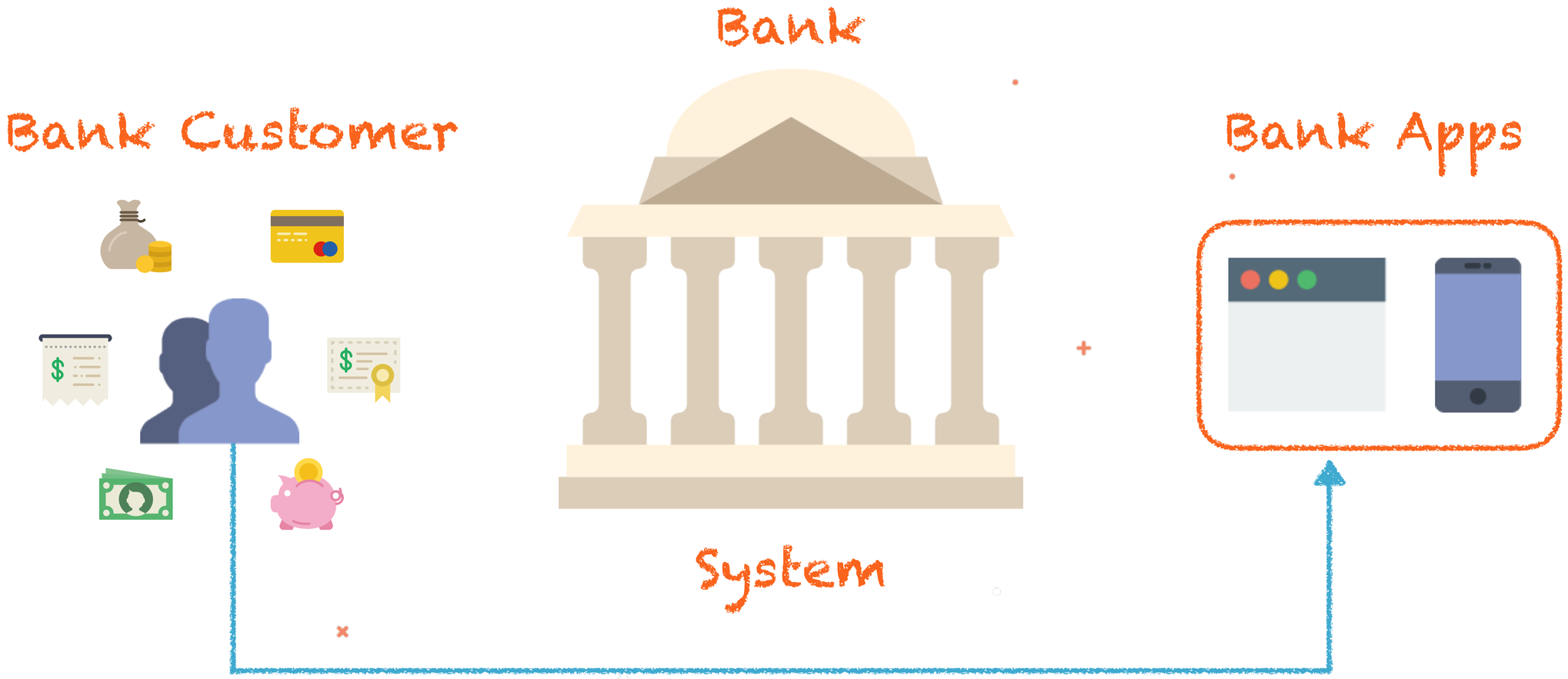
Identity Management (IdM)

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

IdM: Provisioning



Actor = User

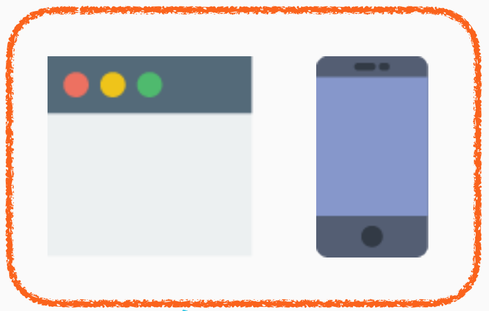


Actor ≠ User

Bank

Bank Customer

Bank Apps

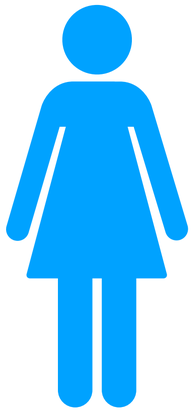
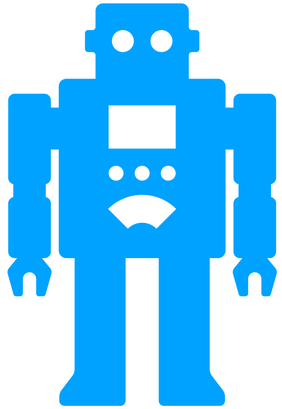
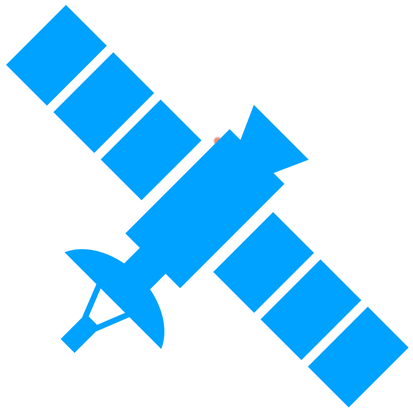
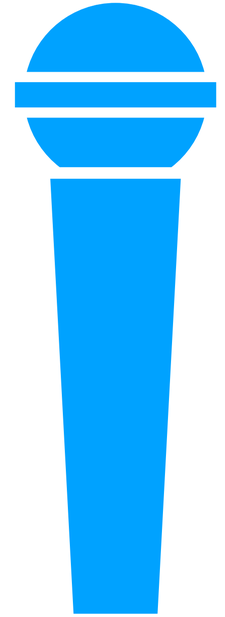


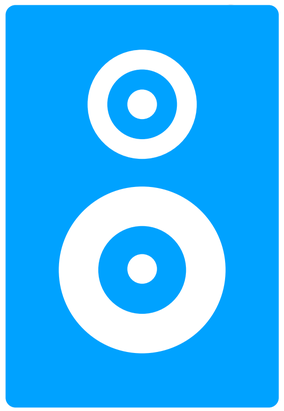
System

(company) Customer

Counter

IdM: Provisioning




@itrjwyss

AMBASSADOR

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

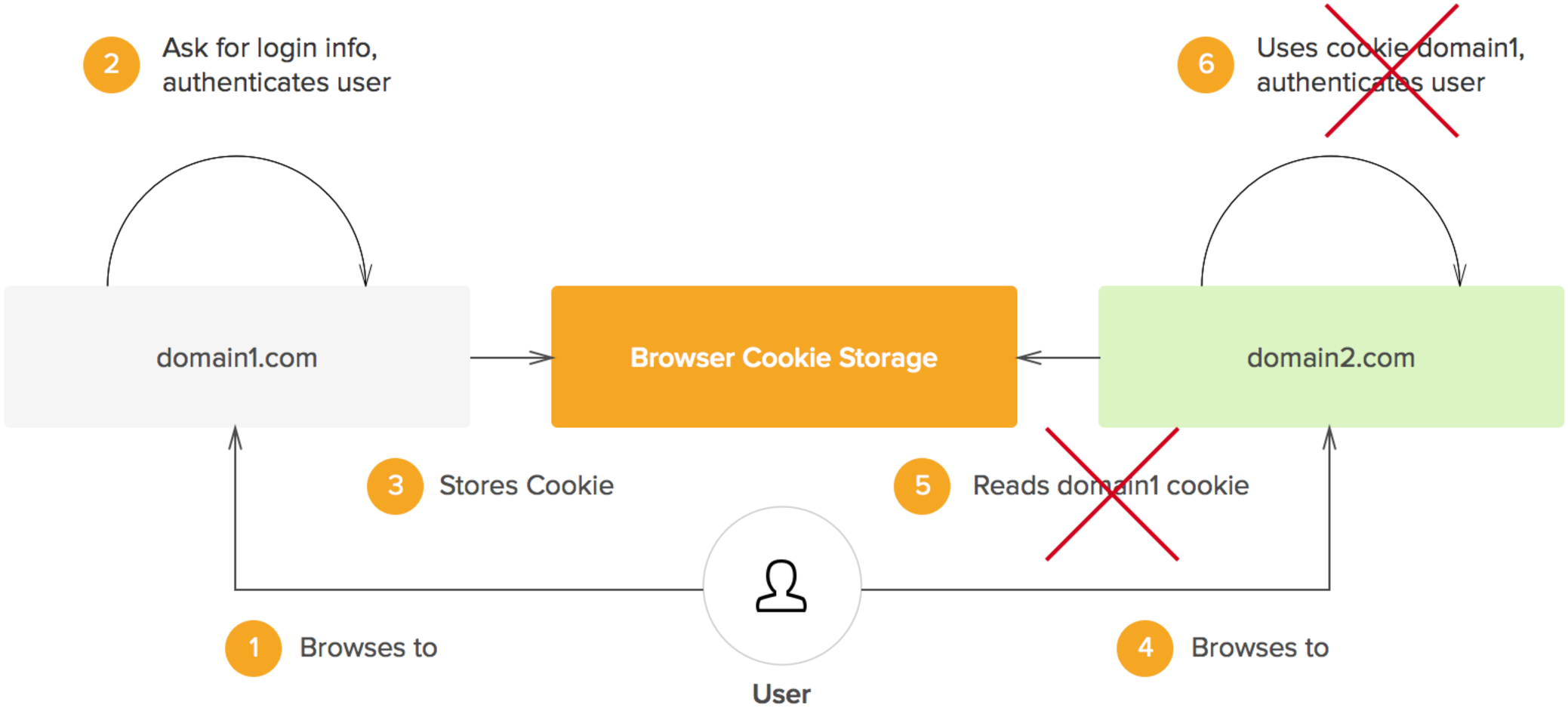
IAM: Authorization

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

IAM: Identity Federation

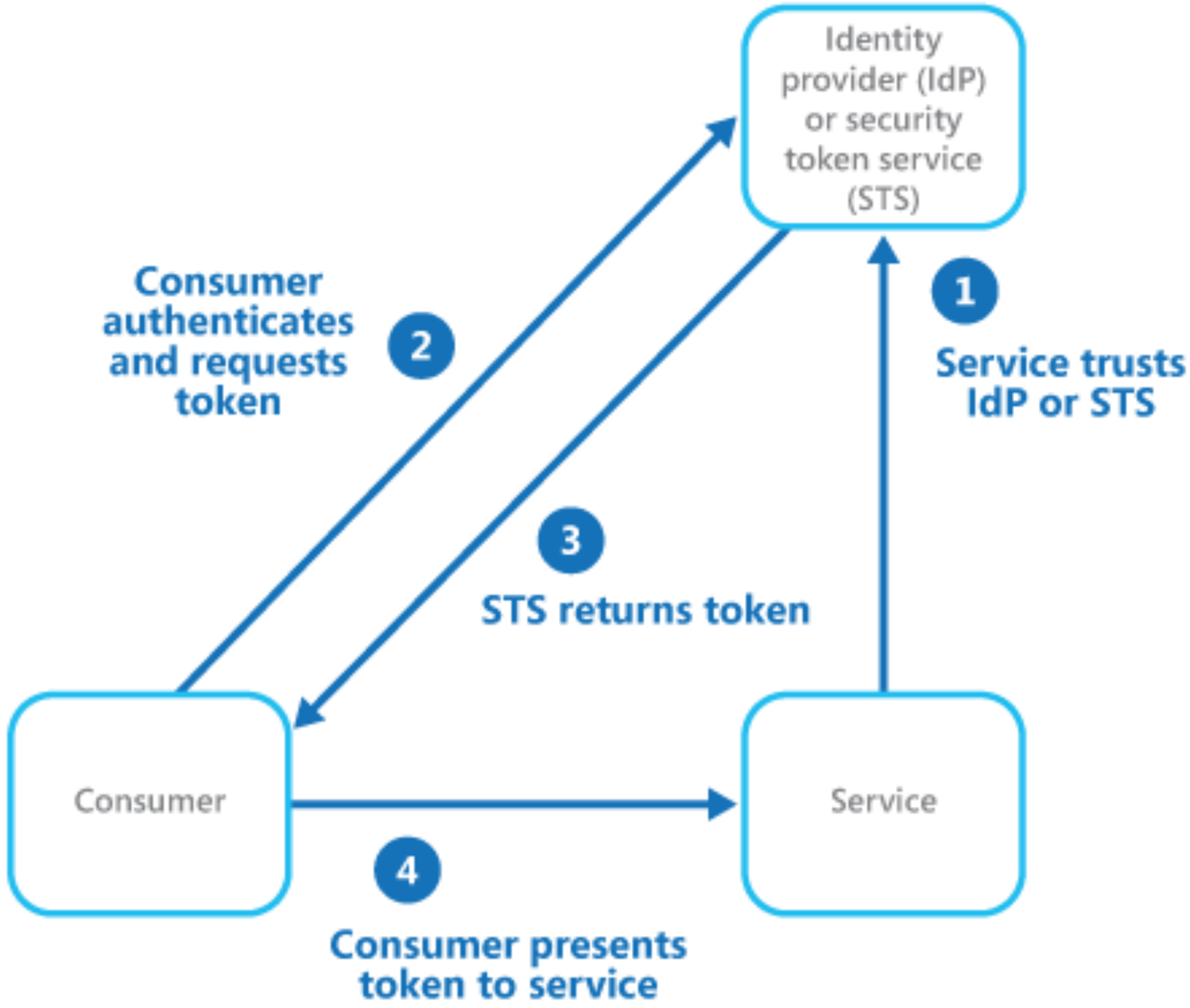
- Ensuring users can use the same identification data to access resources on related domains.

SAME-ORIGIN-POLICY FORBIDS THIS



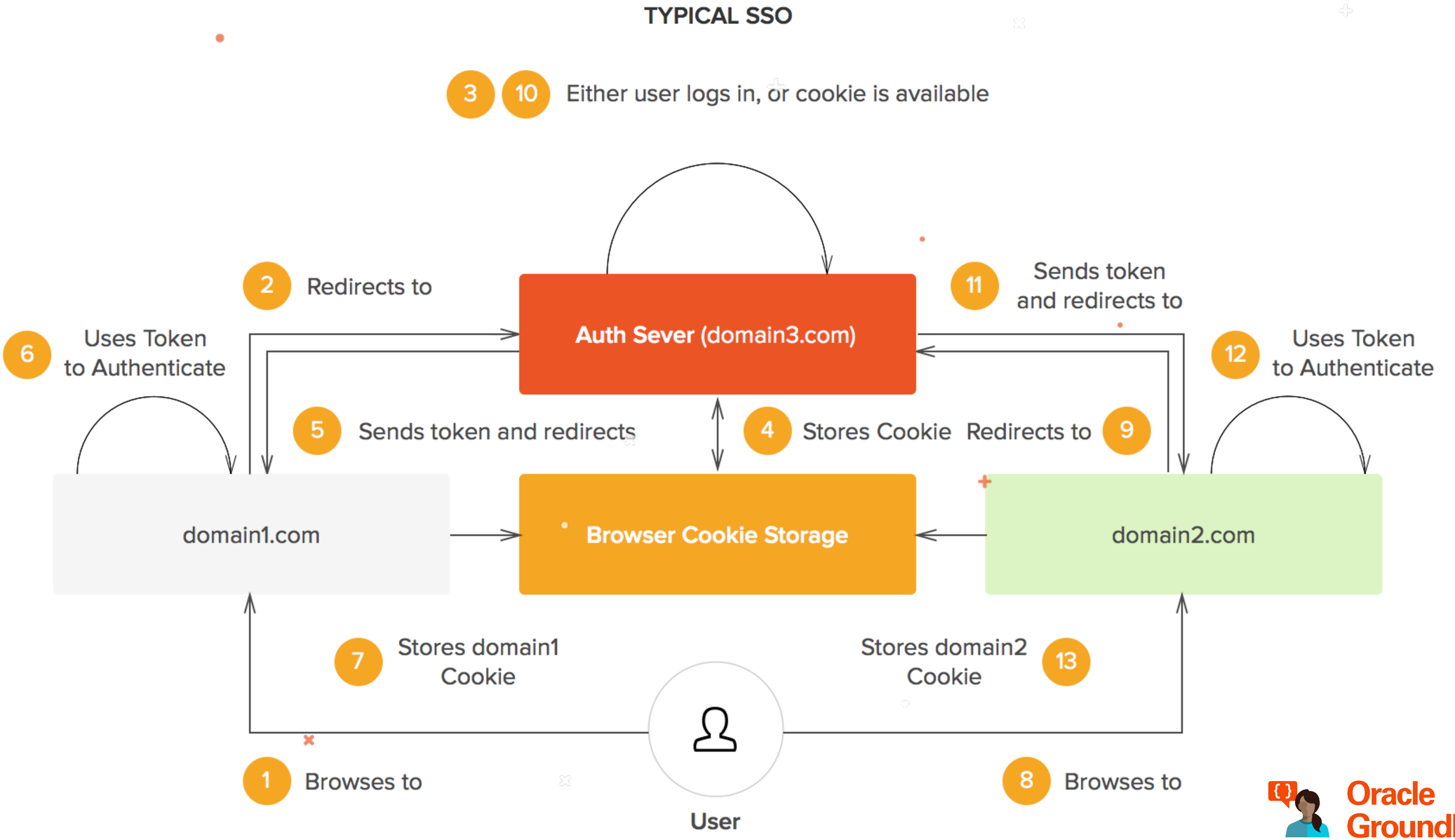
Federated Identity

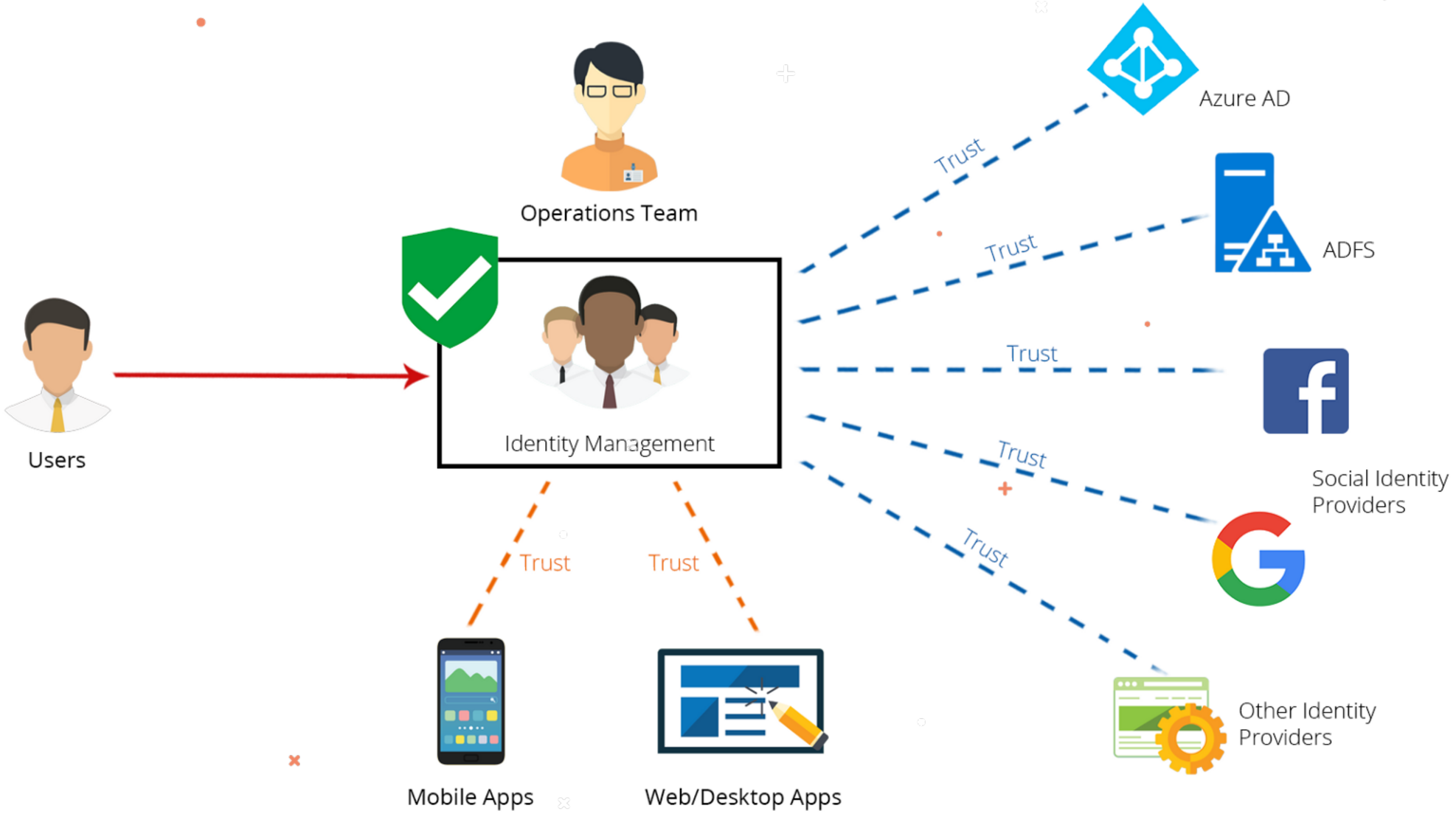
- In some way, are methods of transferring data without violating the same origin policy.
- This way, if domain X and Y are related, and their owners want users to move freely between the two, they can simply triangulate around an external authorization server.



@itrjwyss

AMBASSADOR





@itrjwyss

AMBASSADOR

Social Federated Identity

@itrjwyss

Oracle Groundbreaker Ambassador

Basecamp

Amazon Web Services

AOL Reader

Auth0 OpenIDConnect

Baidu

Bitbucket

Box

Docomo

@itrjwyss

Dropbox

Dwolla

Evernote

Exact

Facebook

Fitbit

Github

Goodreads

Google

Instagram

LinkedIn

Microsoft Account

miiCard

Generic OAuth2 Provider

PayPal

Planning Center

@itrjwyss

RenRen

Salesforce

Shopify

SoundCloud

The City

Twitter

vKontakte

Weibo

@itrjwyss

Oracle Groundbreaker Ambassador

WordPress

Yahoo!

Yammer

Yandex

@itrjwyss

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

Norwegian BankID

Swedish BankID

NEM ID

Danish NemID

@itrjwyss

IAM: Authentication

- Ensuring that a given user is the user they identify as
  - Single Sign-On (SSO)
  - Multi-factor Authentication (MFA)
  - Passwordless
  - *Federated Identity (Management)*

IAM: Authentication

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

IAM: Authentication

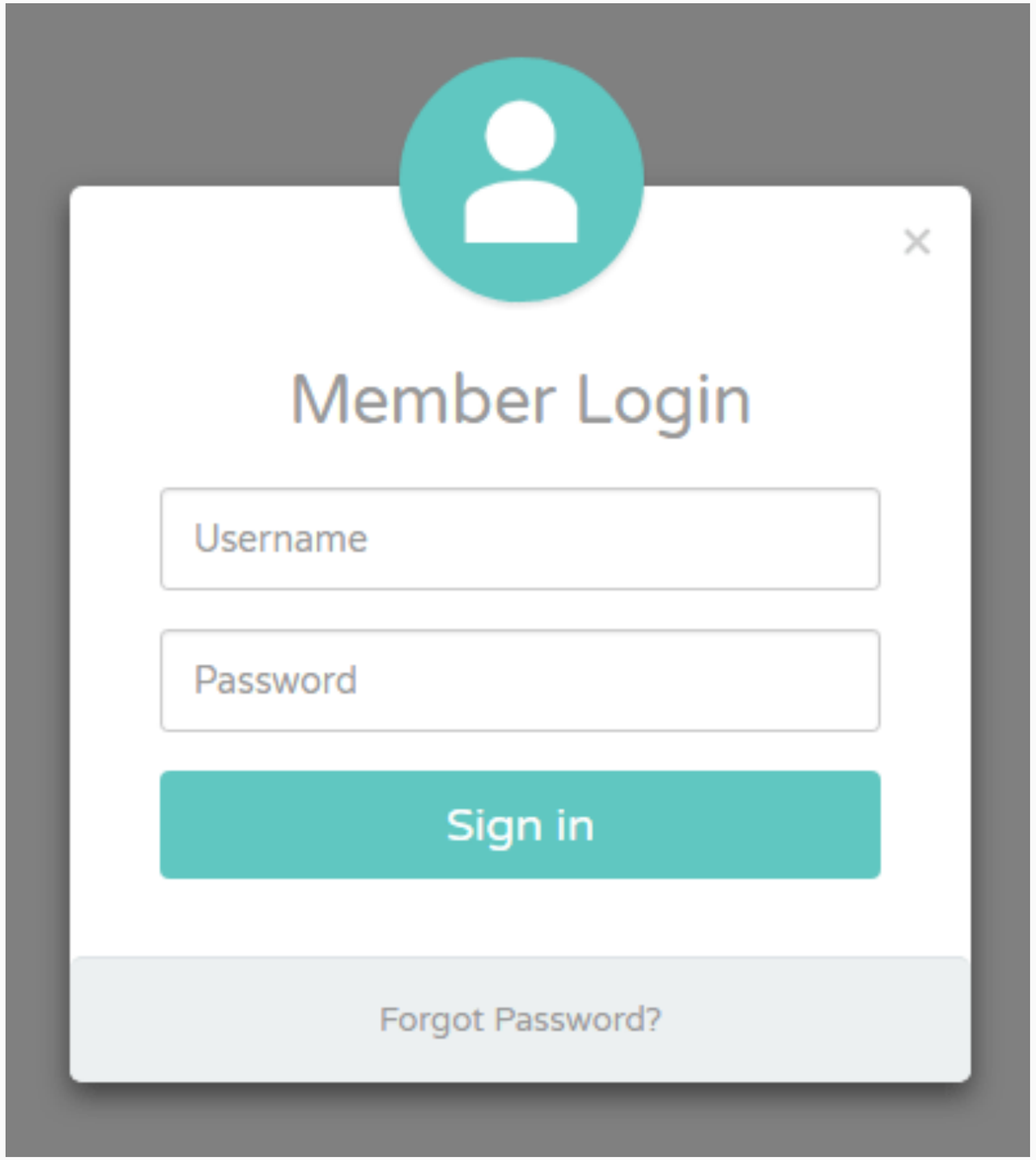
- Ensuring that a given user is the user they identify as
  - Single Sing-On (SSO)
  - Multi-factor Authentication (MFA)
  - Passwordless
  - *Federated Identity (Management)*

Knowledge

Possession

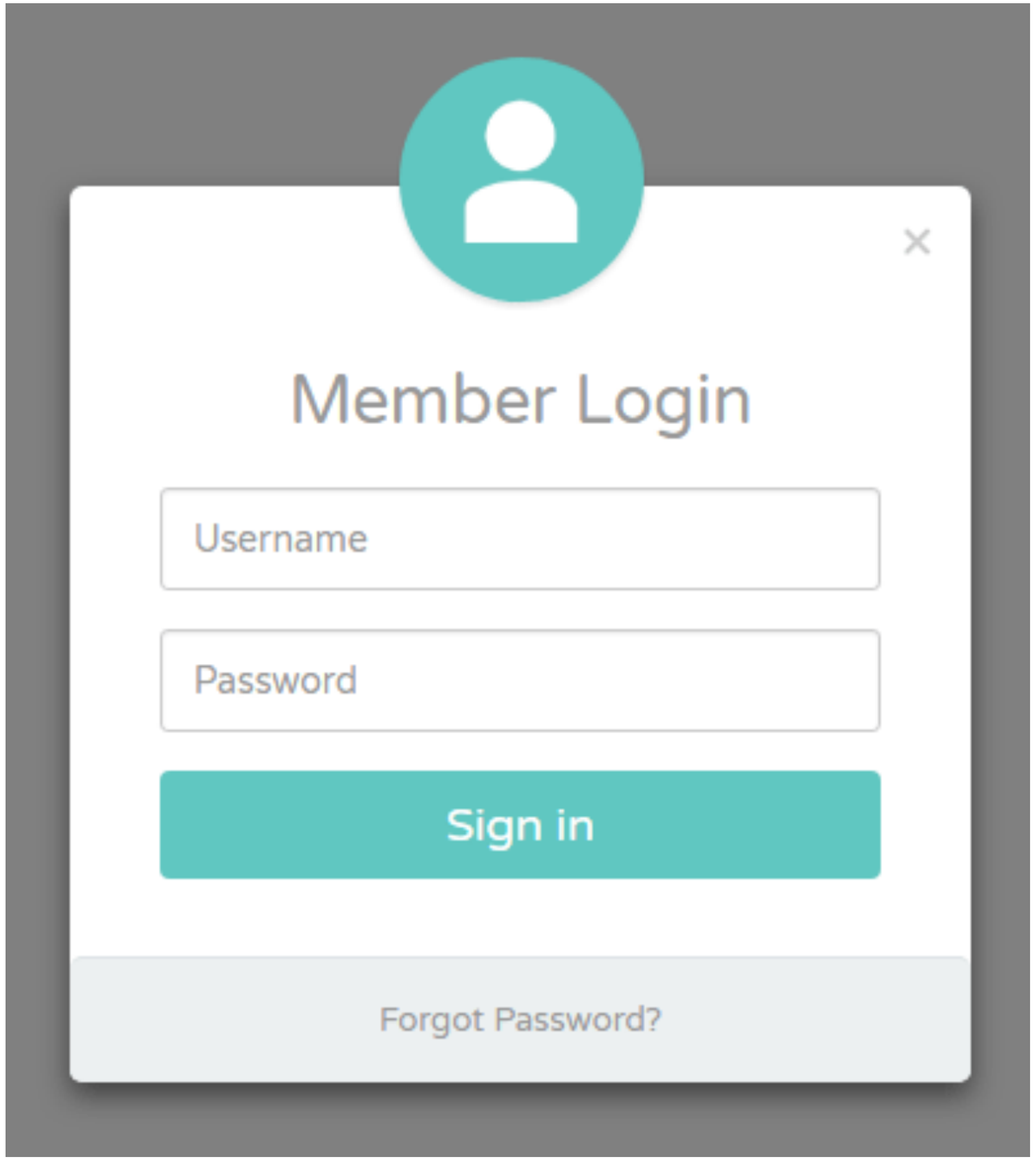
Biometric

@itrjwyss



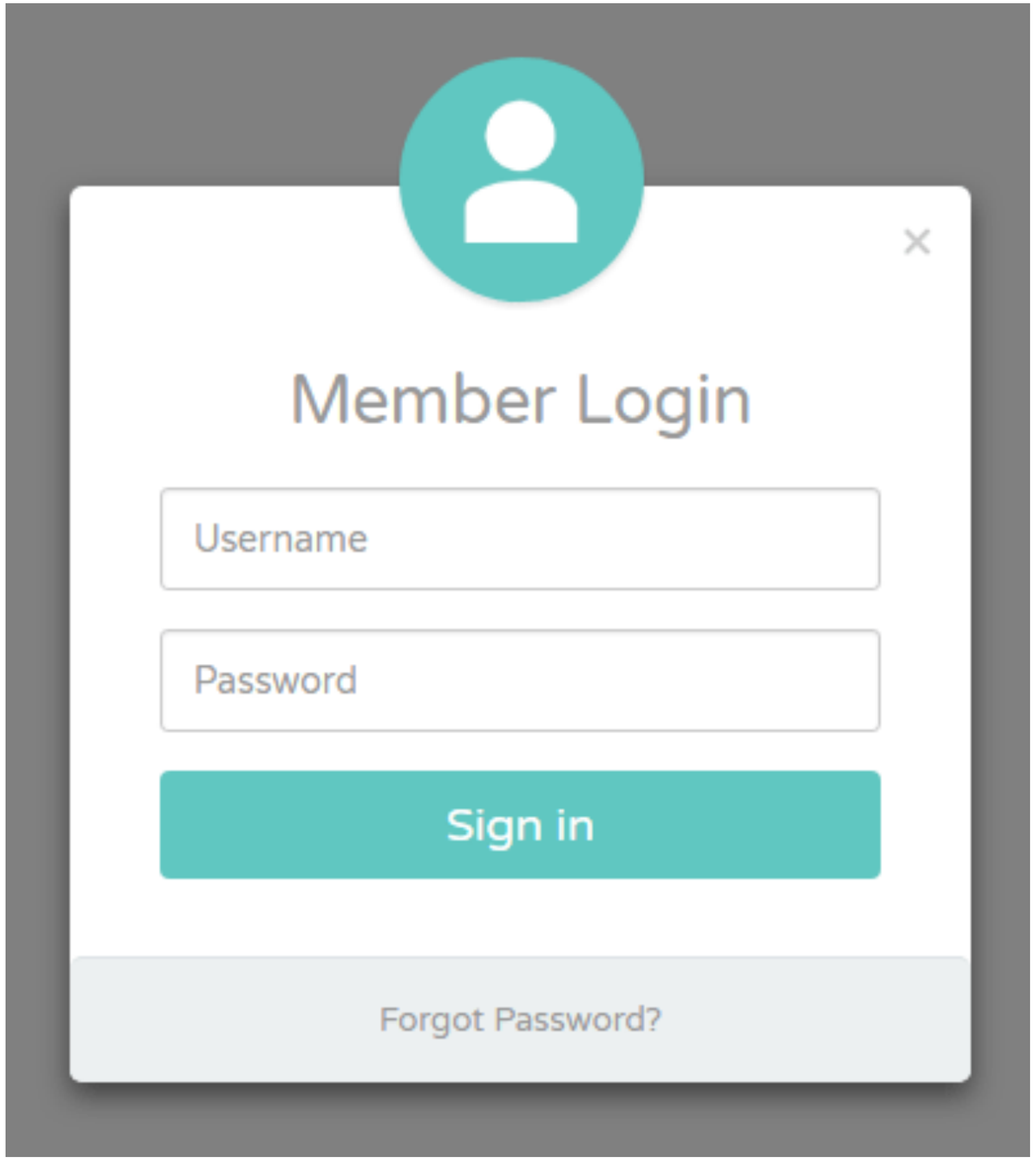
@itrjwyss

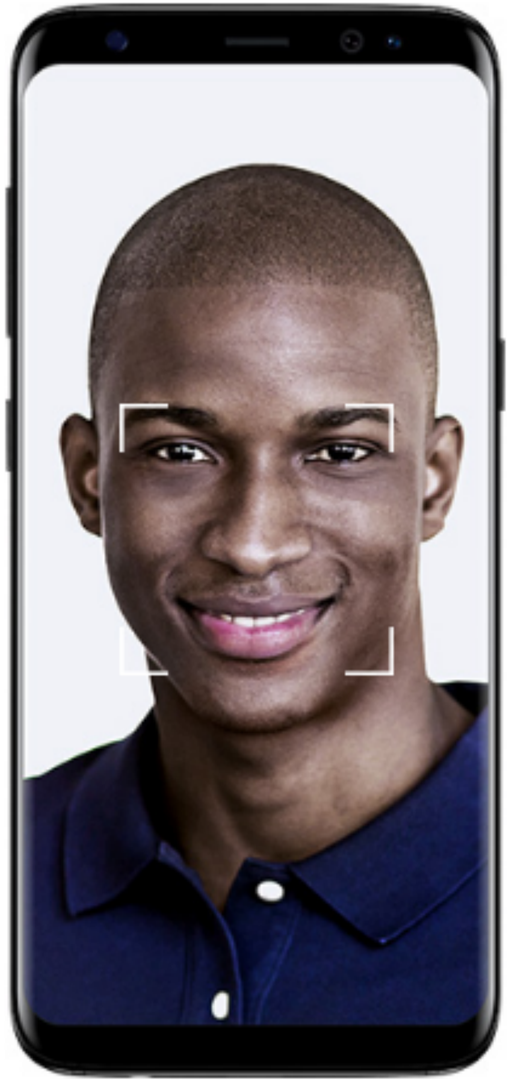
Oracle Groundbreaker Ambassador



@itrjwyss

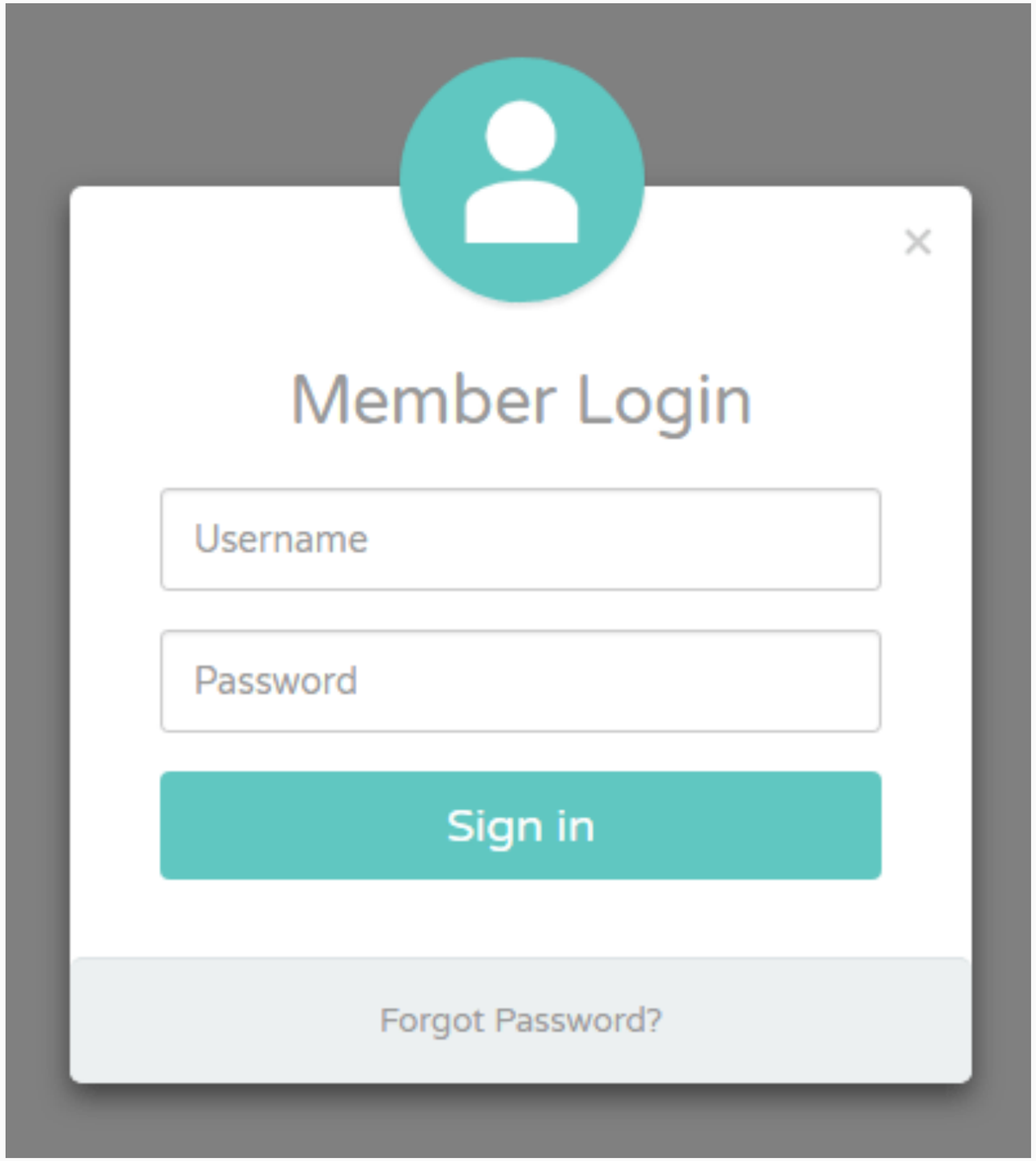
Oracle Groundbreaker Ambassador





@itrjwyss

Oracle Groundbreaker Ambassador



@itrjwyss

Oracle Groundbreaker Ambassador

MFA | Multi-Factor Authentication

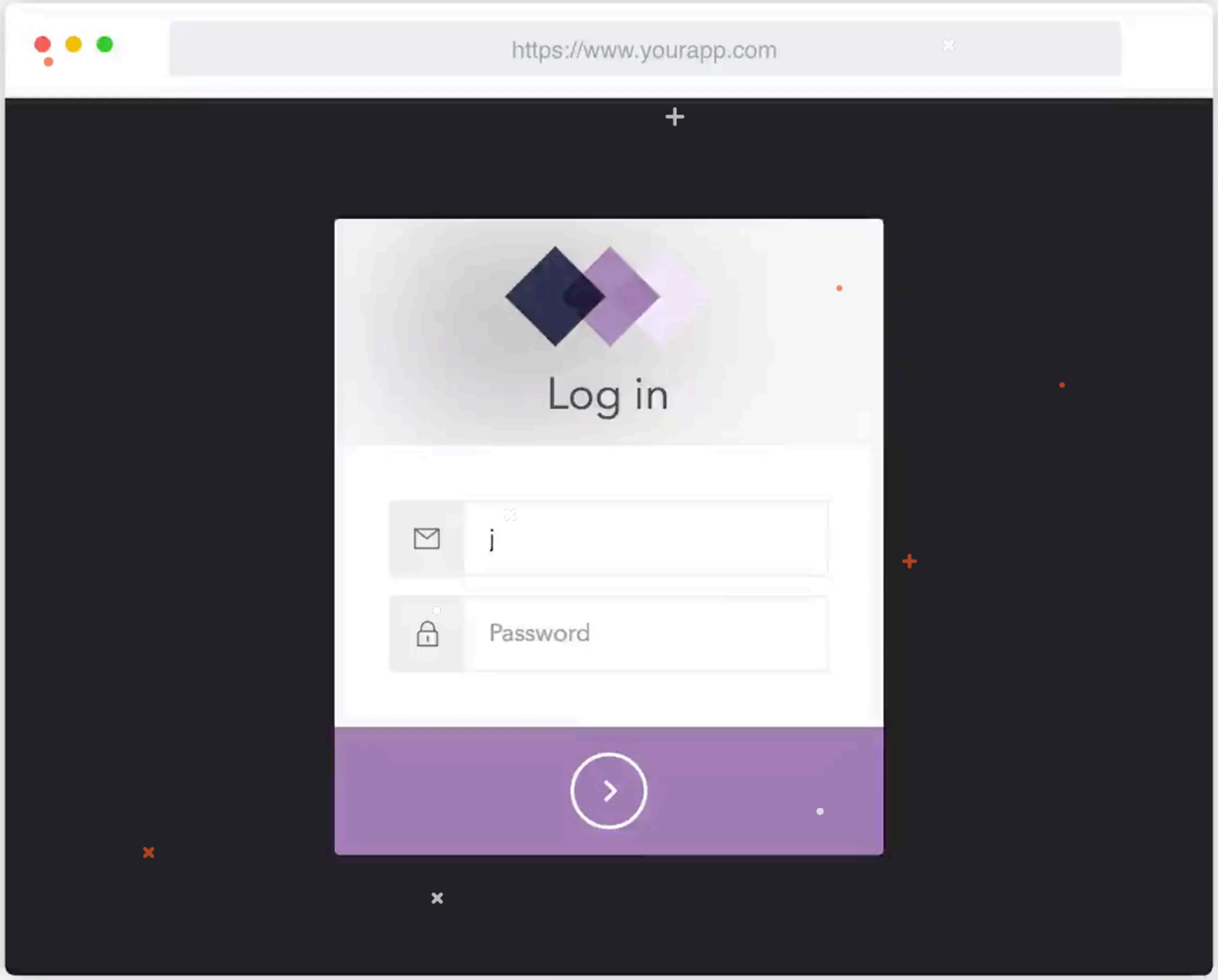
@itrjwyss

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



AMBASSADOR

MFA: Biometrics

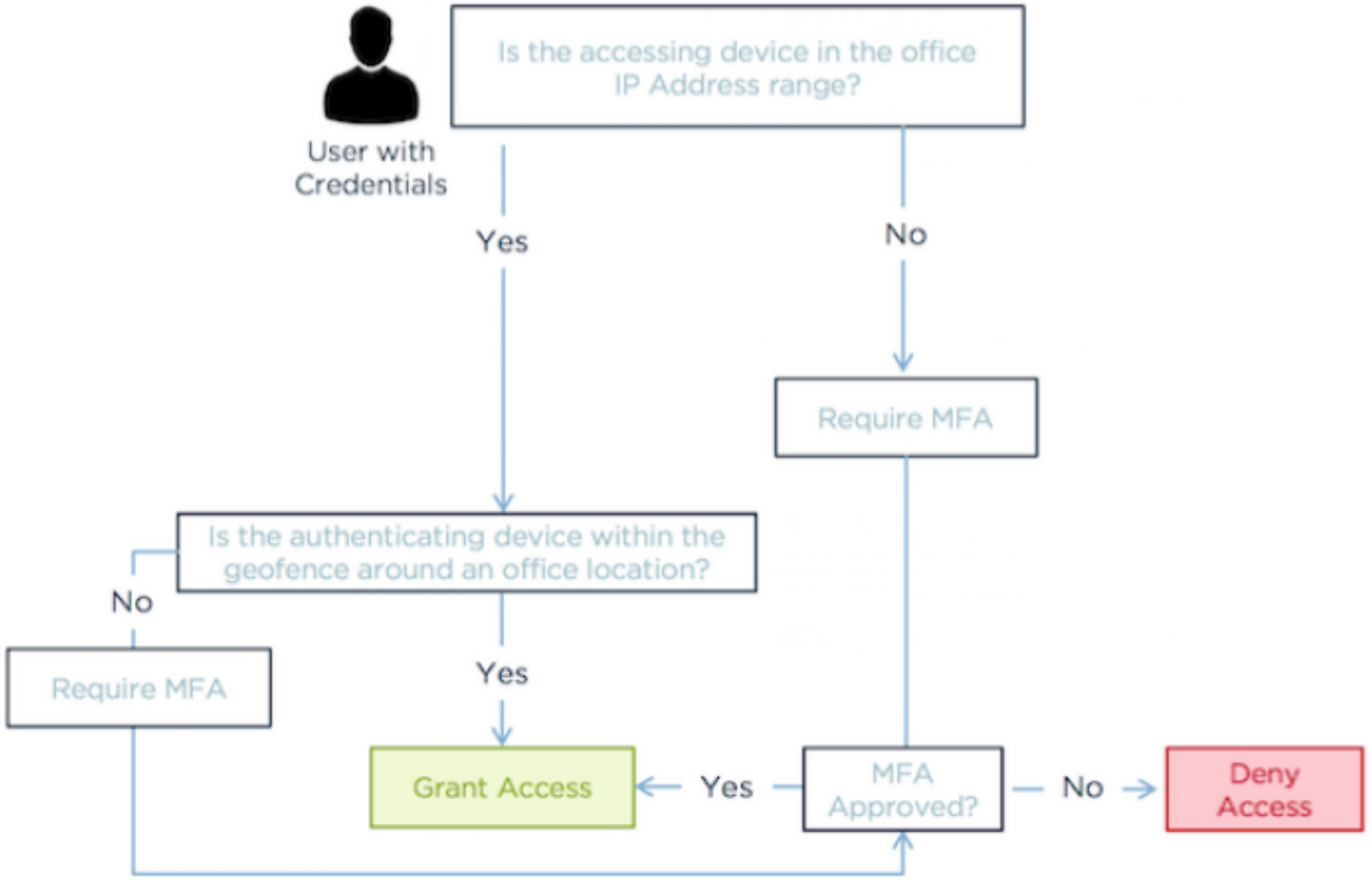
- Common methods are touch ID (fingerprint), facial recognition.
- We can have other ones:
    - Iris or retina recognition
    - Voice recognition (Twilio)
    - Typing recognition
    - DNA usage

MFA: Biometrics

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

Passwordless

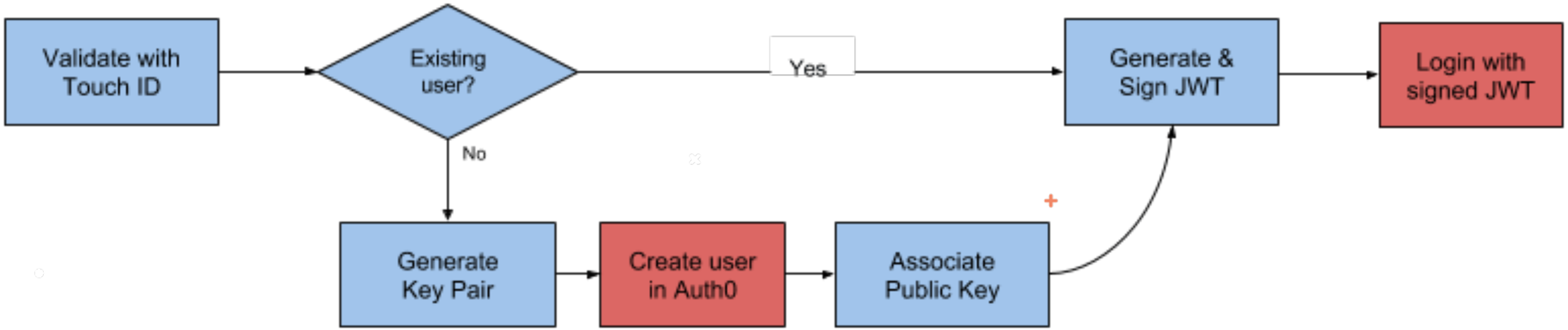
- It means authenticating a user by means other than having them type in a password
- Can also evaluate user and device contexts to provide authentication methods.



@itrjwyss

Oracle Groundbreaker Ambassador

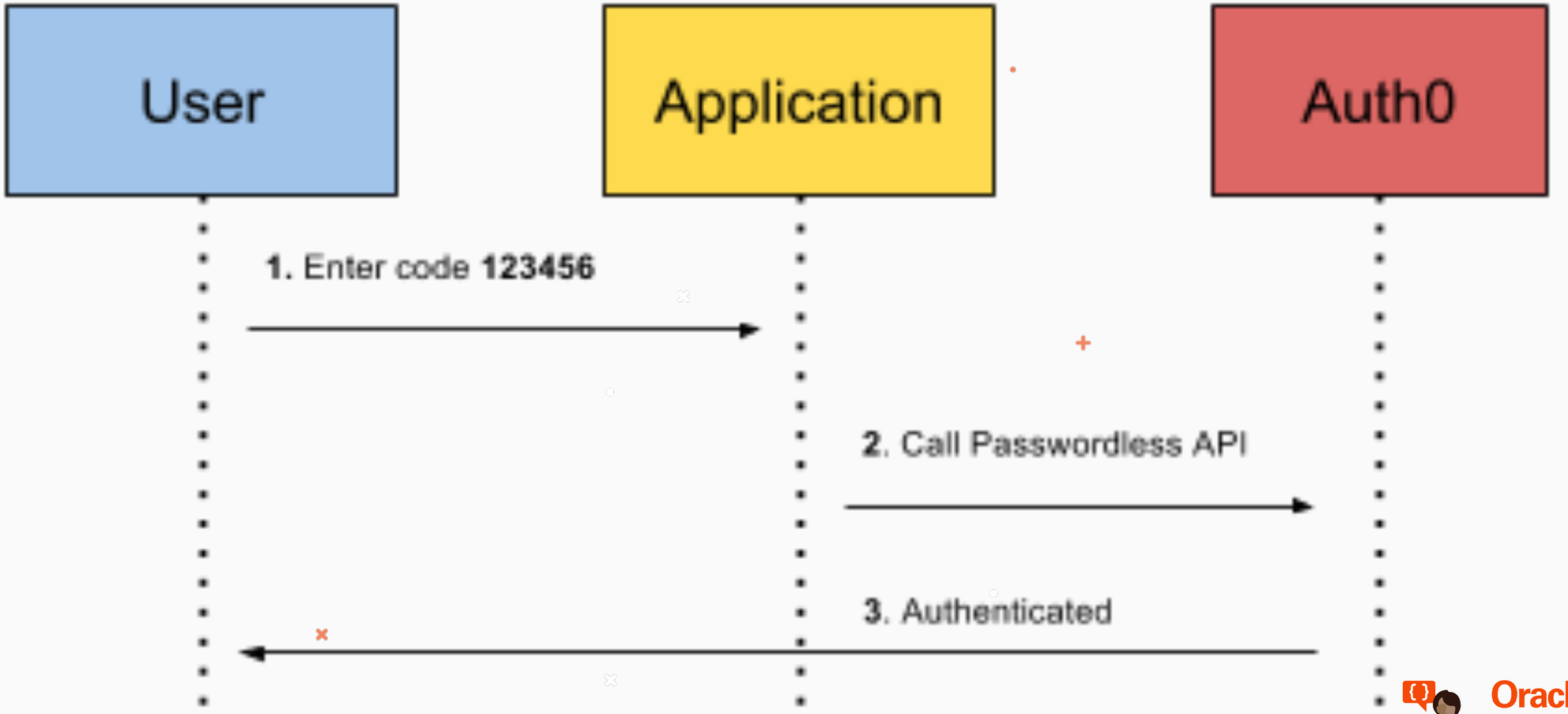
Touch ID



@itrjwyss

AMBASSADOR

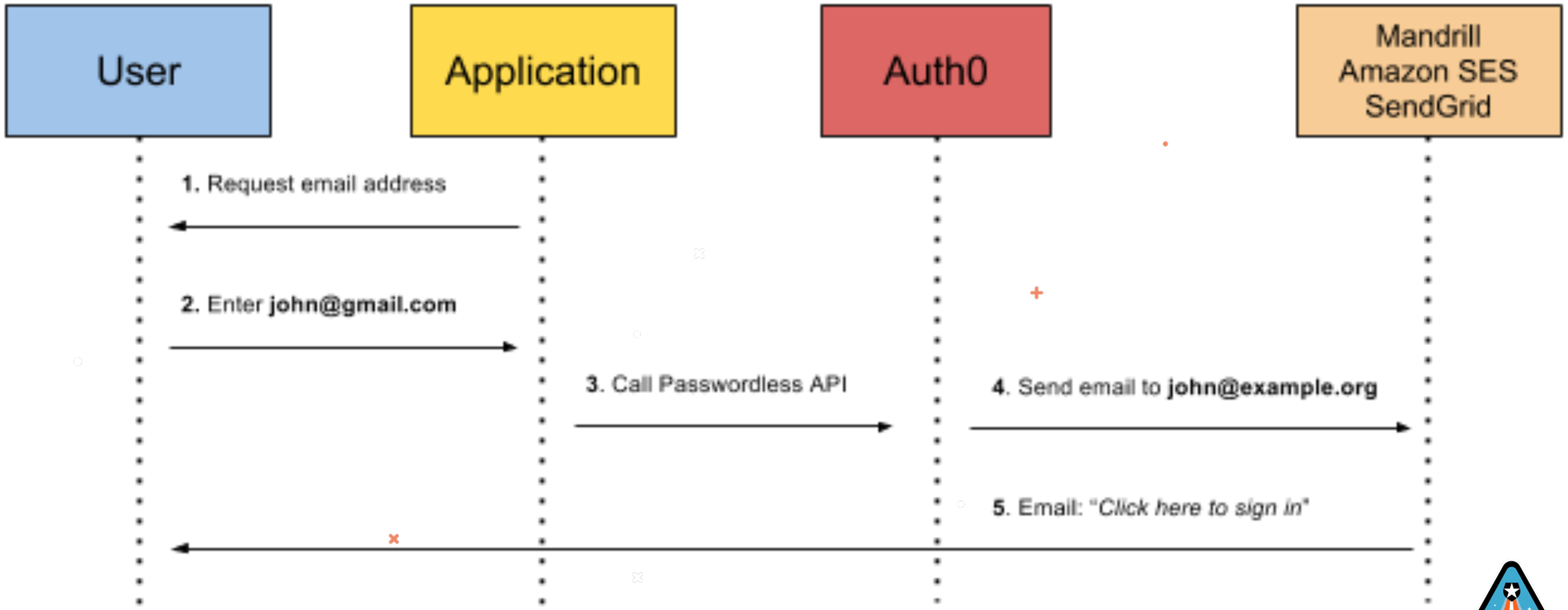
SMS Code



@itrjwyss

Oracle Groundbreaker Ambassador

Magic Link



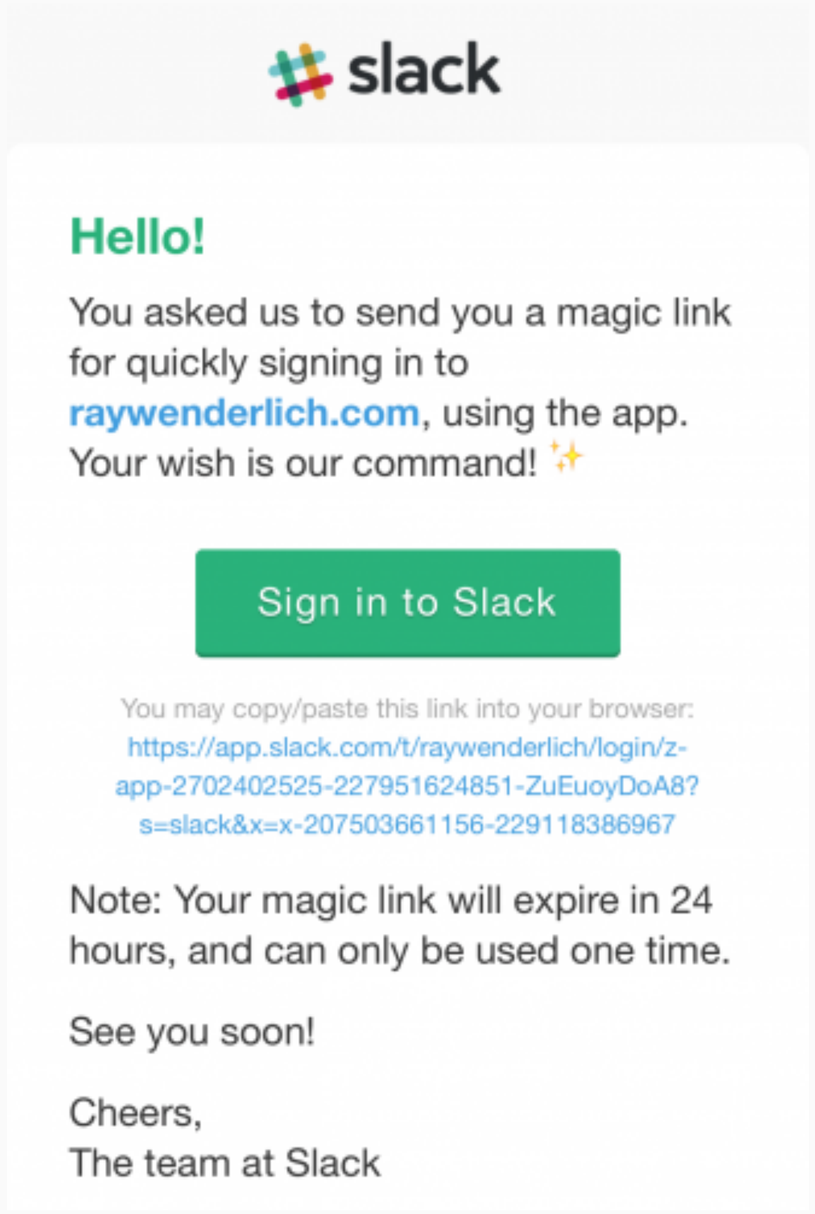
@itrjwyss

AMBASSADOR

slack

@itrjwyss

Oracle
Groundbreaker
Ambassador



@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

@itrjwyss

Oracle
Groundbreaker
Ambassador

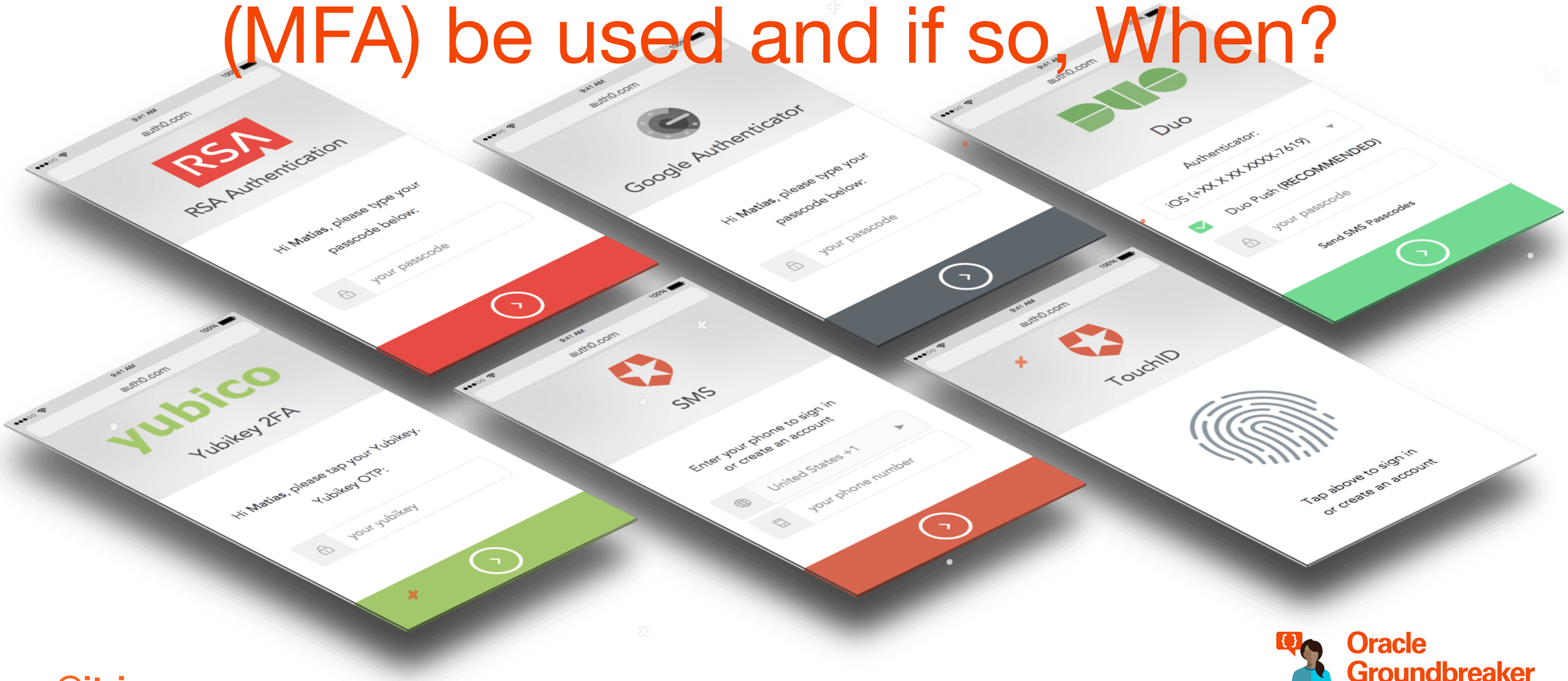
3. Username uniqueness

4. How will users Log In?

@itrjwyss

AMBASSADOR

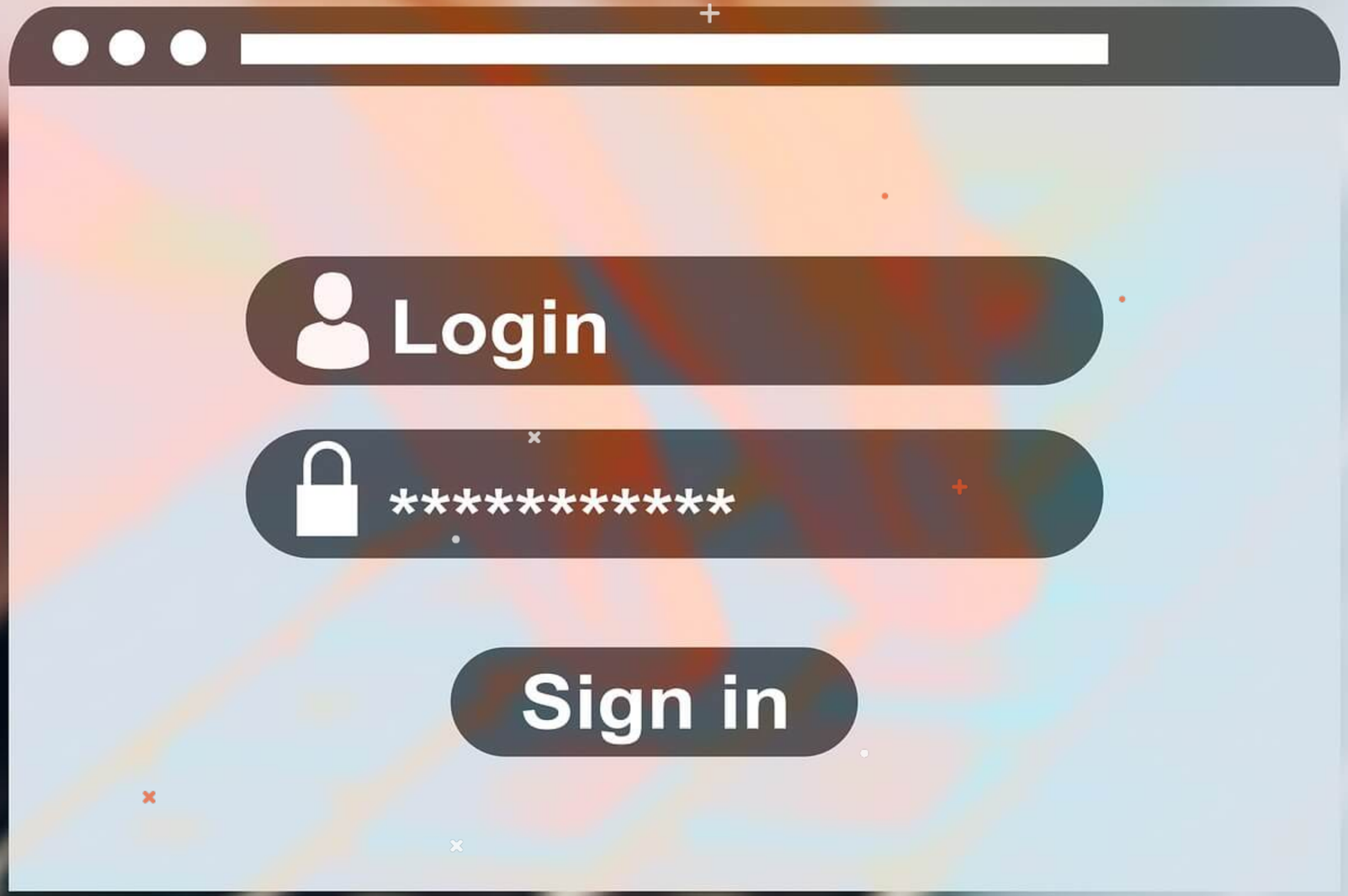
5. Should Multi-Factor Authentication (MFA) be used and if so, When?



@itrjwyss

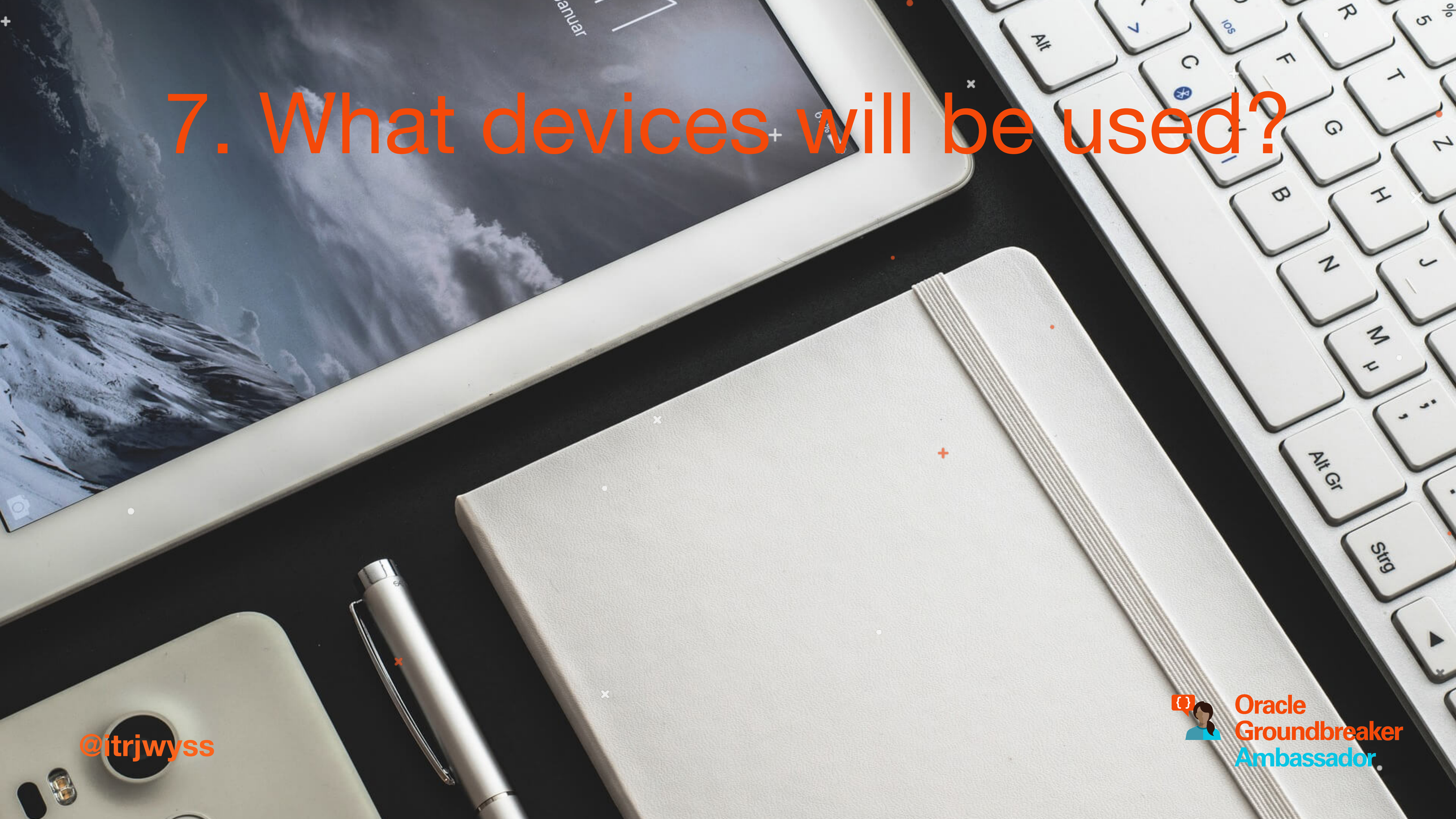
Oracle Groundbreaker Ambassador

6. Is single Sing-On needed?



@itrjwyss

AMBASSADOR



7. What devices will be used?

@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

AMBASSADOR

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

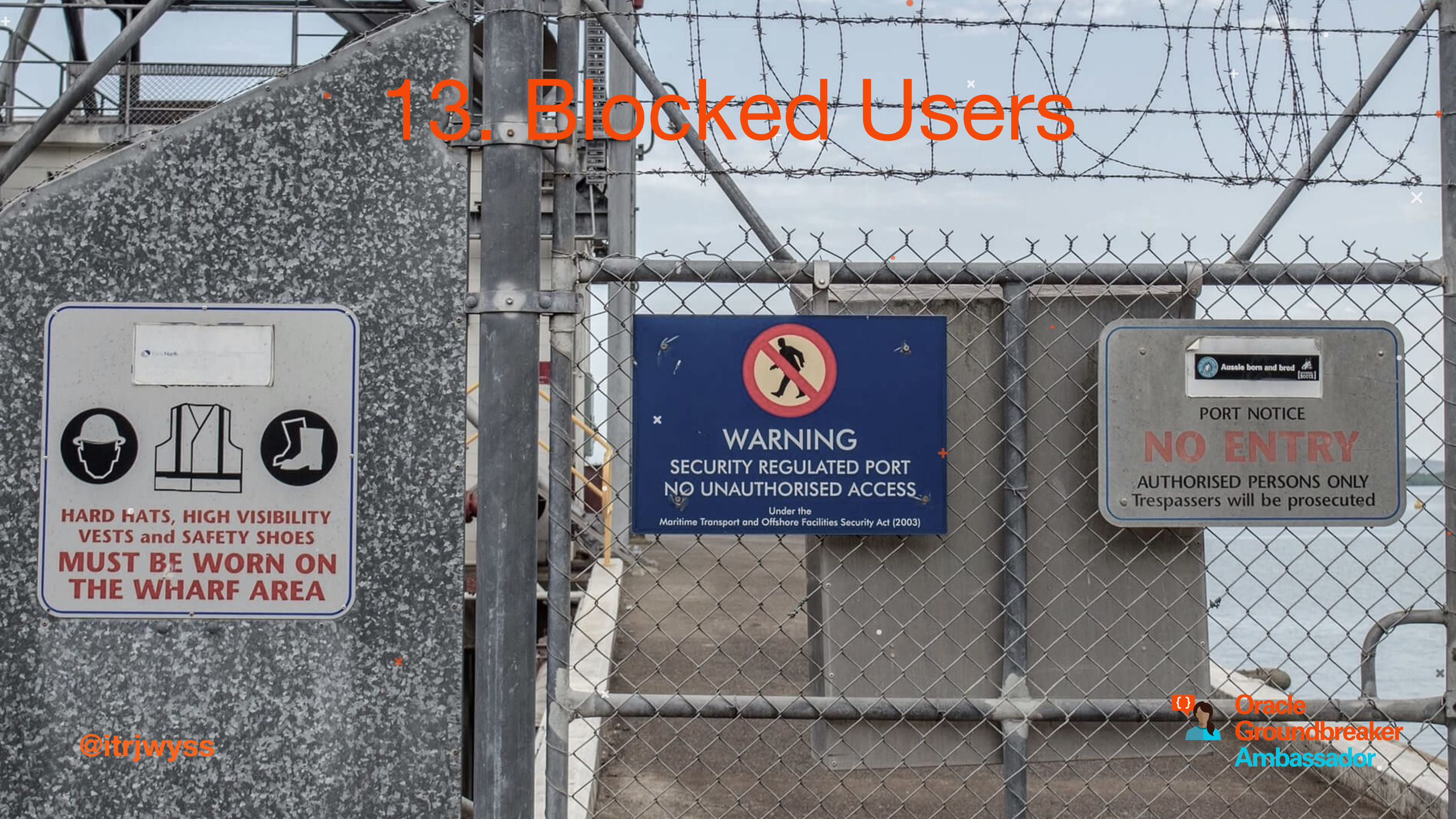
@itrjwyss

Oracle Groundbreaker Ambassador

@itrjwyss

AMBASSADOR

13. Blocked Users



@itrjwyss

Oracle Groundbreaker Ambassador

14. Anomaly Detection

@itrjwyss

AMBASSADOR

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

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

amazon web services

Auth0

Oracle Groundbreaker Ambassador

Other Popular IDaaS

Other IDaaS

@itrjwyss

Oracle Groundbreaker Ambassador

Other Providers

SailPoint
The Power of Identity

INTERMEDIA AppID
ENTERPRISE

ForgeRock Identity Platform™
Identity Management
Based on the OpenIDM Project

miniOrange

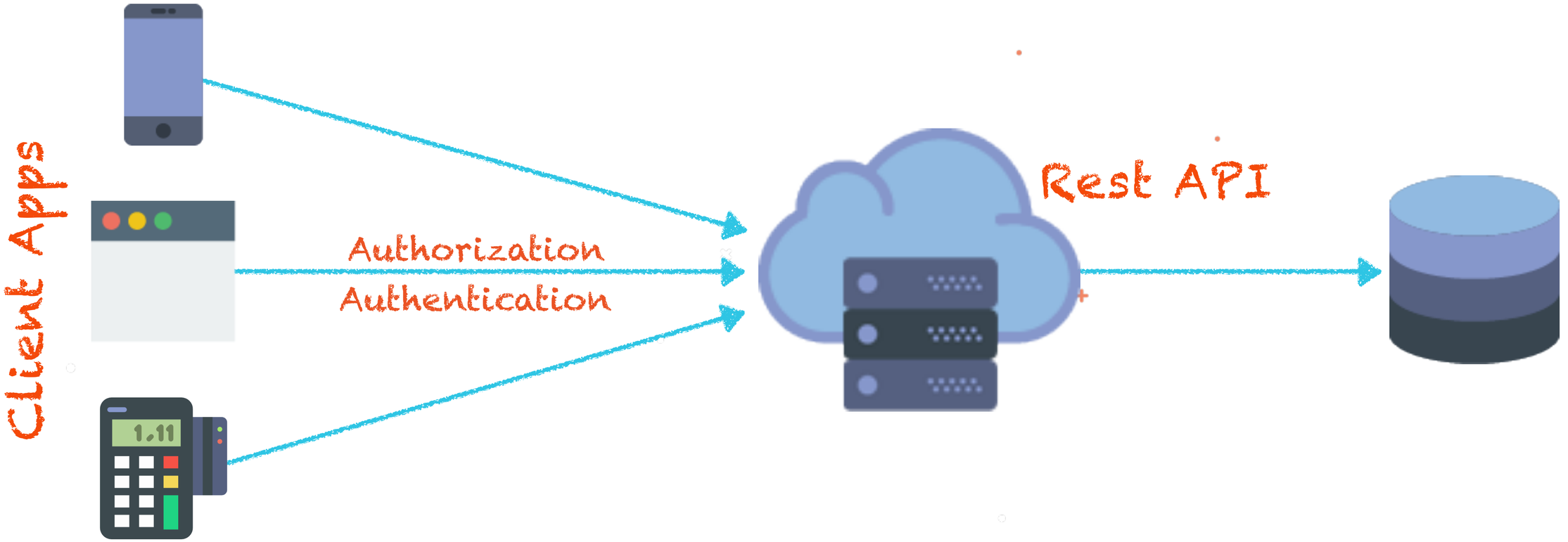
AMBASSADOR

Architecture Level

@itrjwyss

Oracle
Groundbreaker
Ambassador

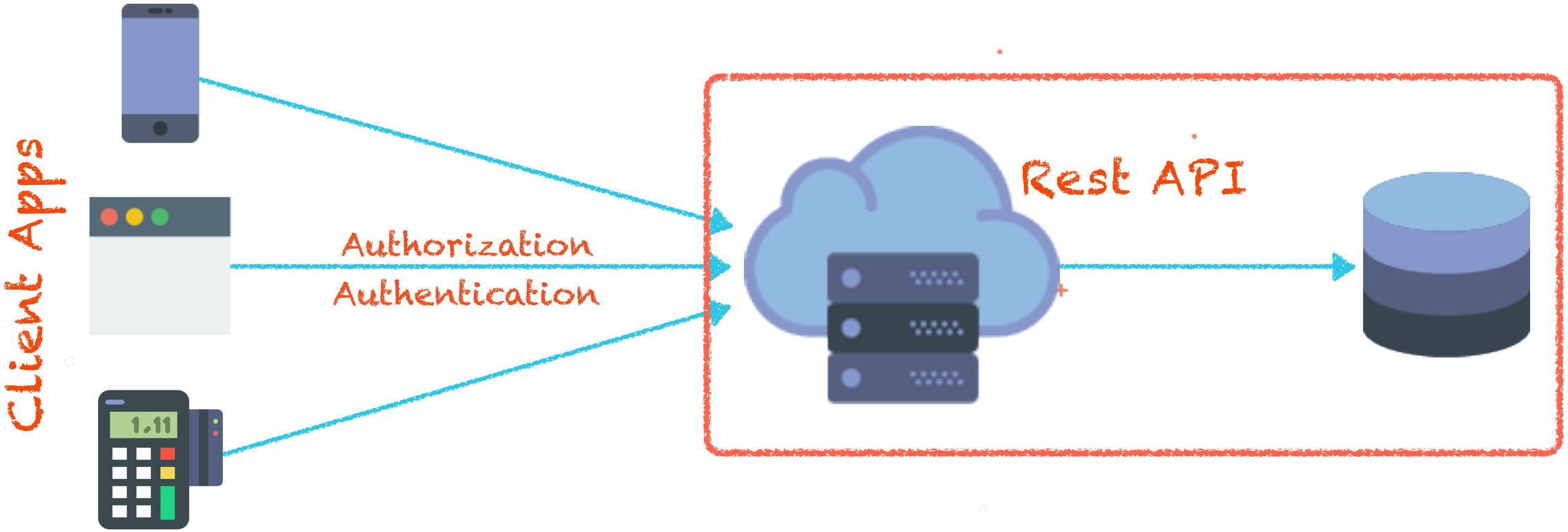
Developing REST APIs



@itrjwyss

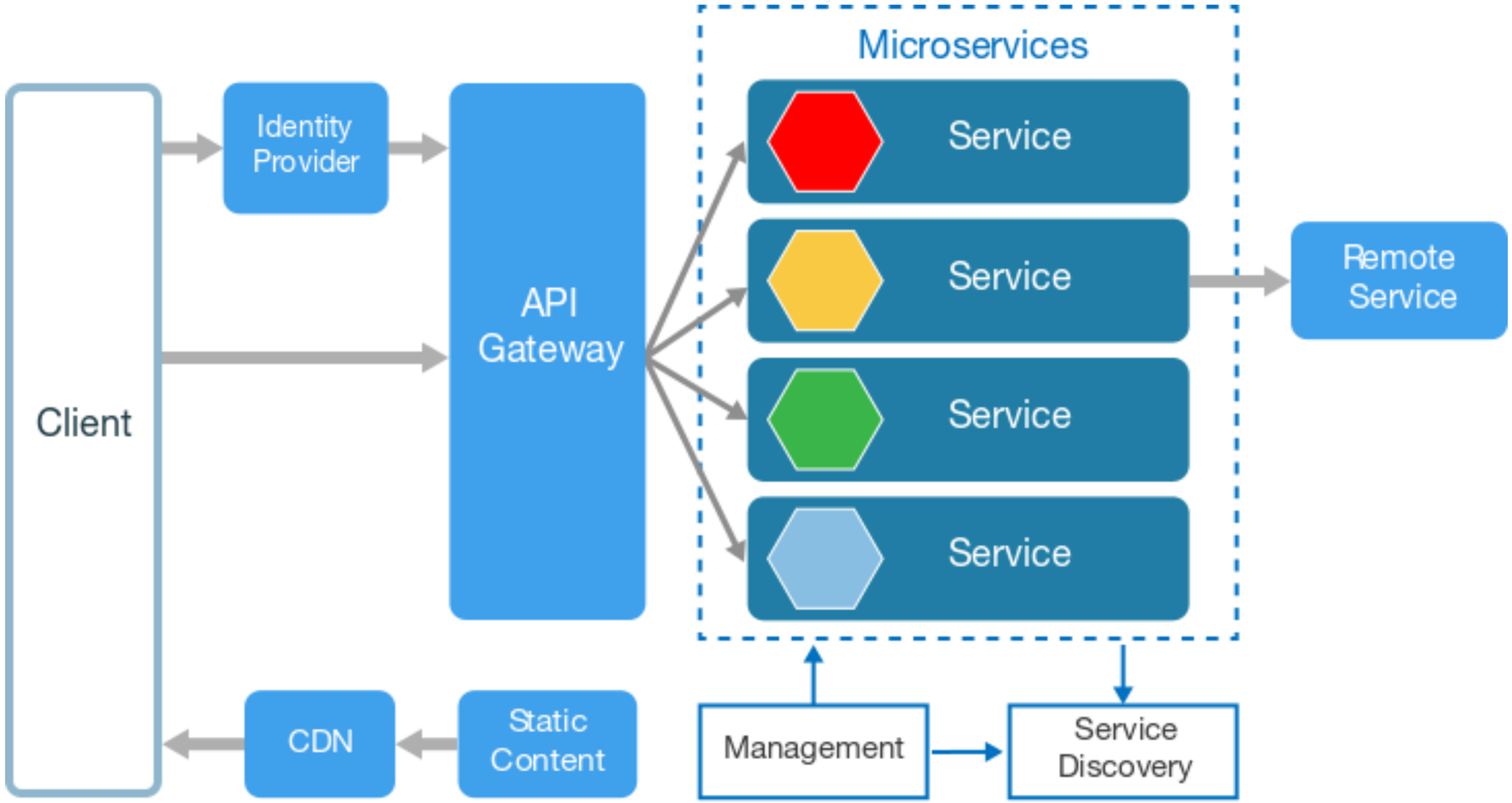
AMBASSADOR

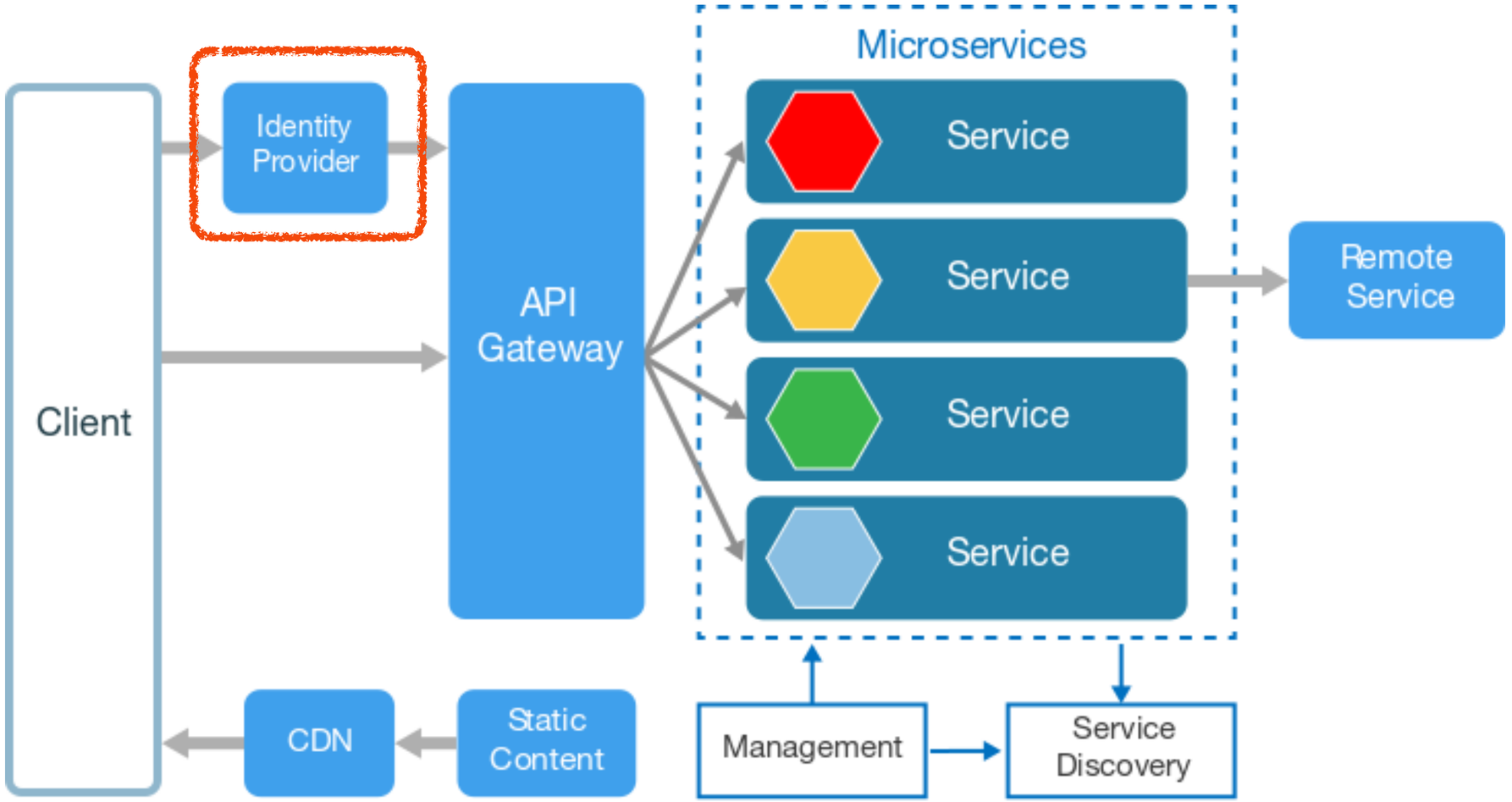
Developing REST APIs

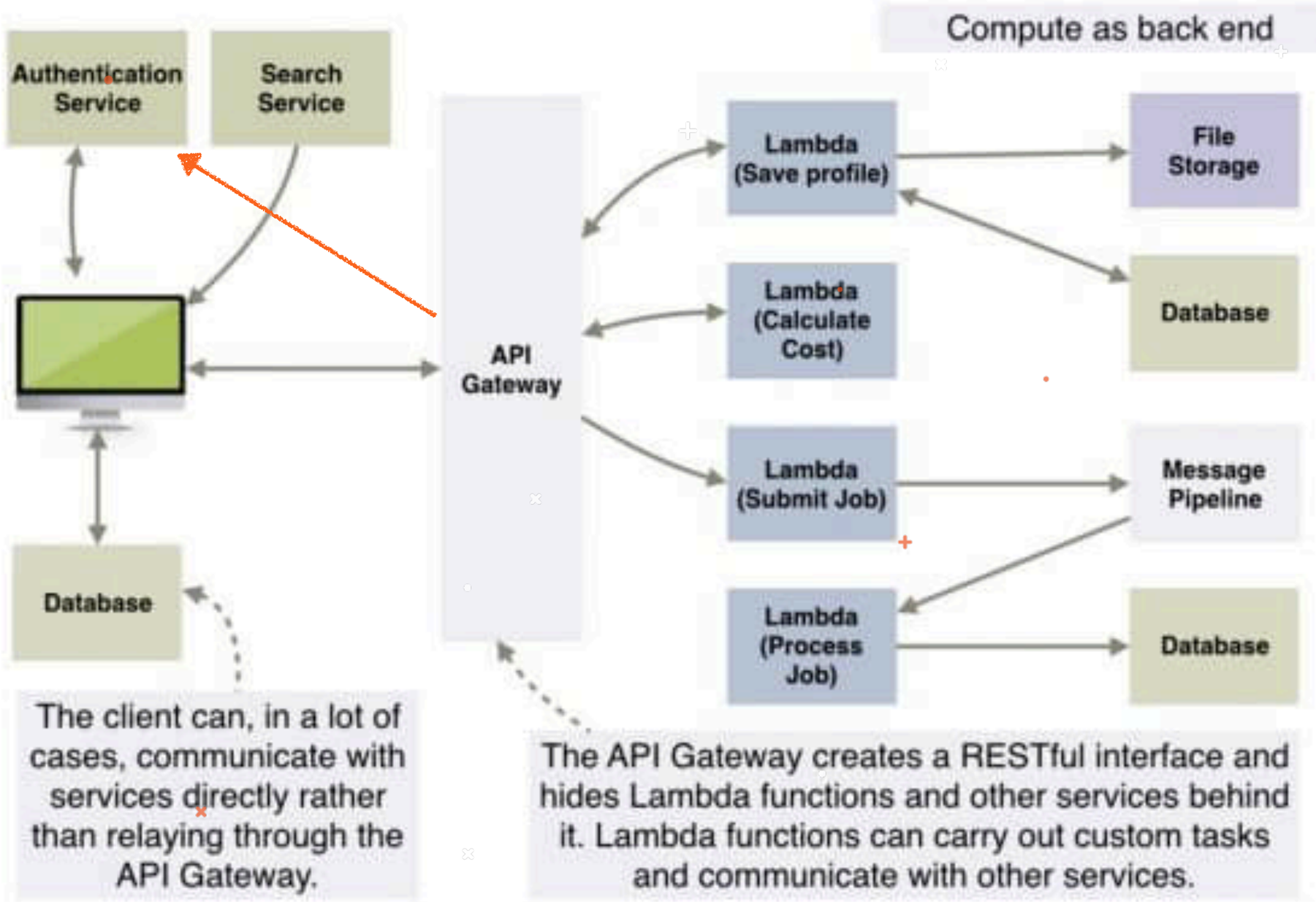


@itrjwyss

AMBASSADOR


Microservices
Client
Identity Provider
API Gateway
Service
Service
Service
Service
Remote Service
CDN
Static Content
Management
Service Discovery


Microservices
Identity Provider
API Gateway
Client
Service
Service
Service
Service
Remote Service
CDN
Static Content
Management
Service Discovery



@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

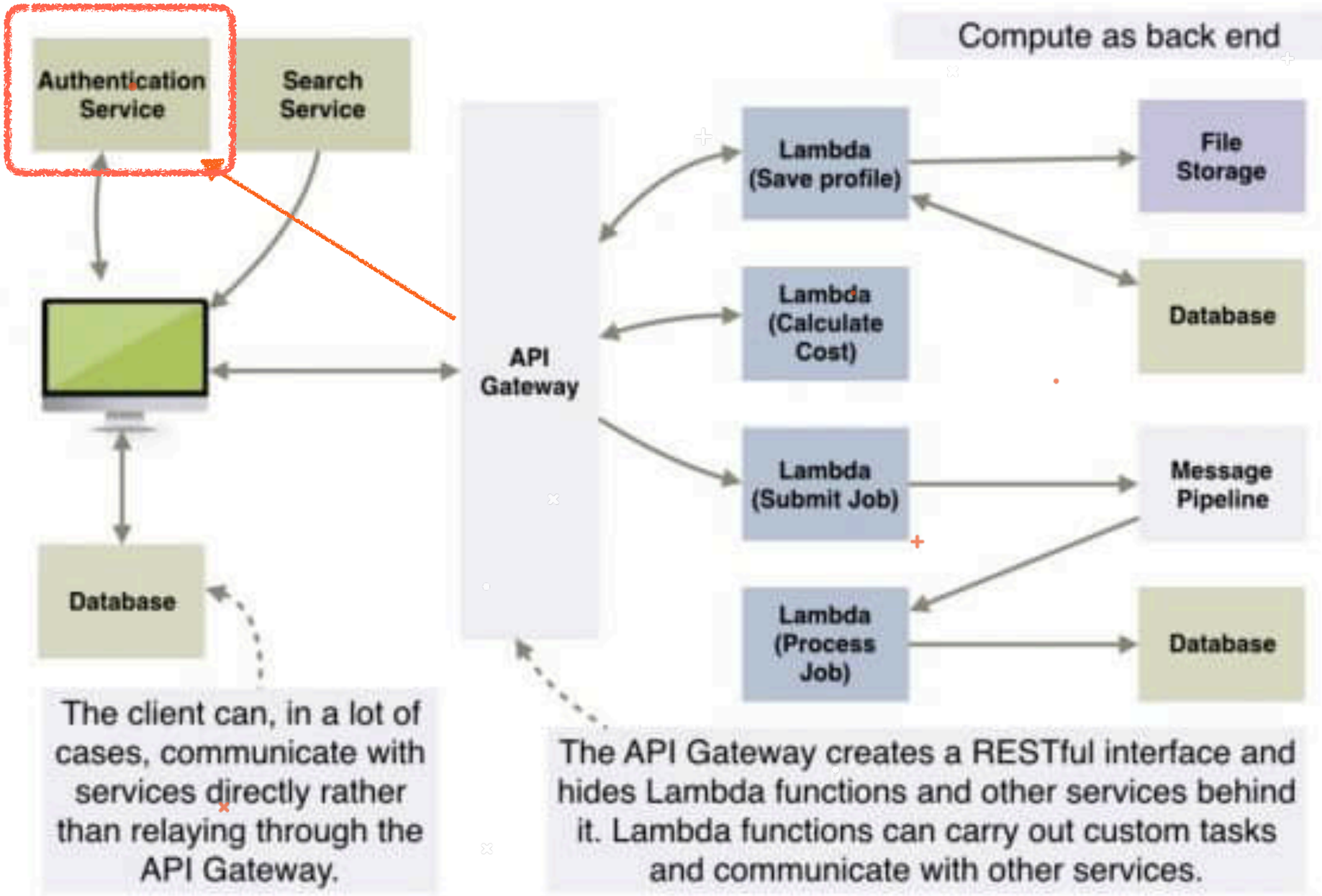


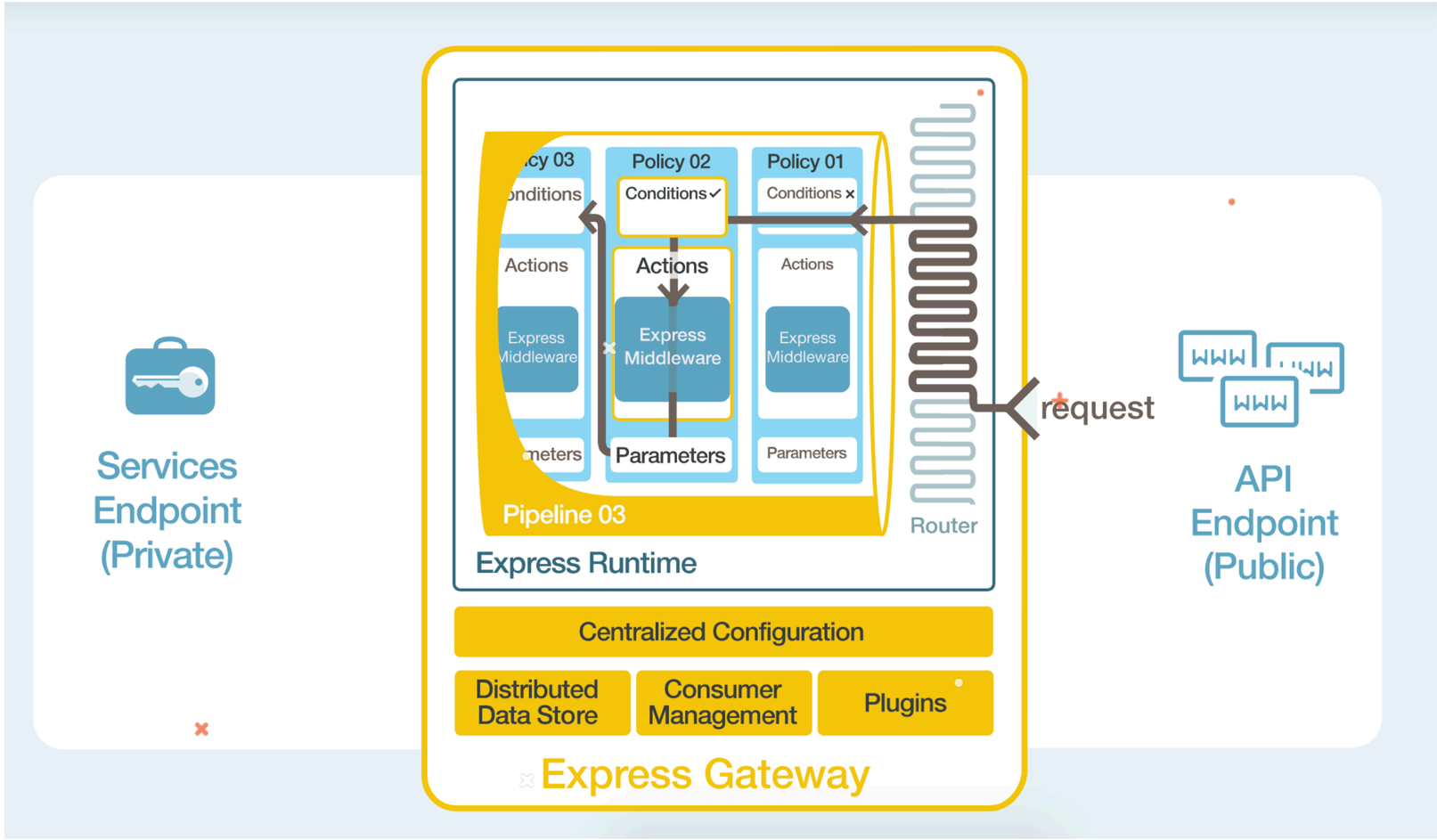
Figure 2: The front end can communicate with services directly and invoke Lambda functions through the API Gateway (Sbarski, Serverless Architectures on AWS, 2016).

Practical Case

@itrjwyss

Oracle
Groundbreaker
Ambassador

Express Gateway



@itrjwyss

AMBASSADOR

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

https://www.facebook.com/itrjwyss

@itrjwyss