

Modern Identity Management

in the era of Serverless and Microservices

VERSION 1.6

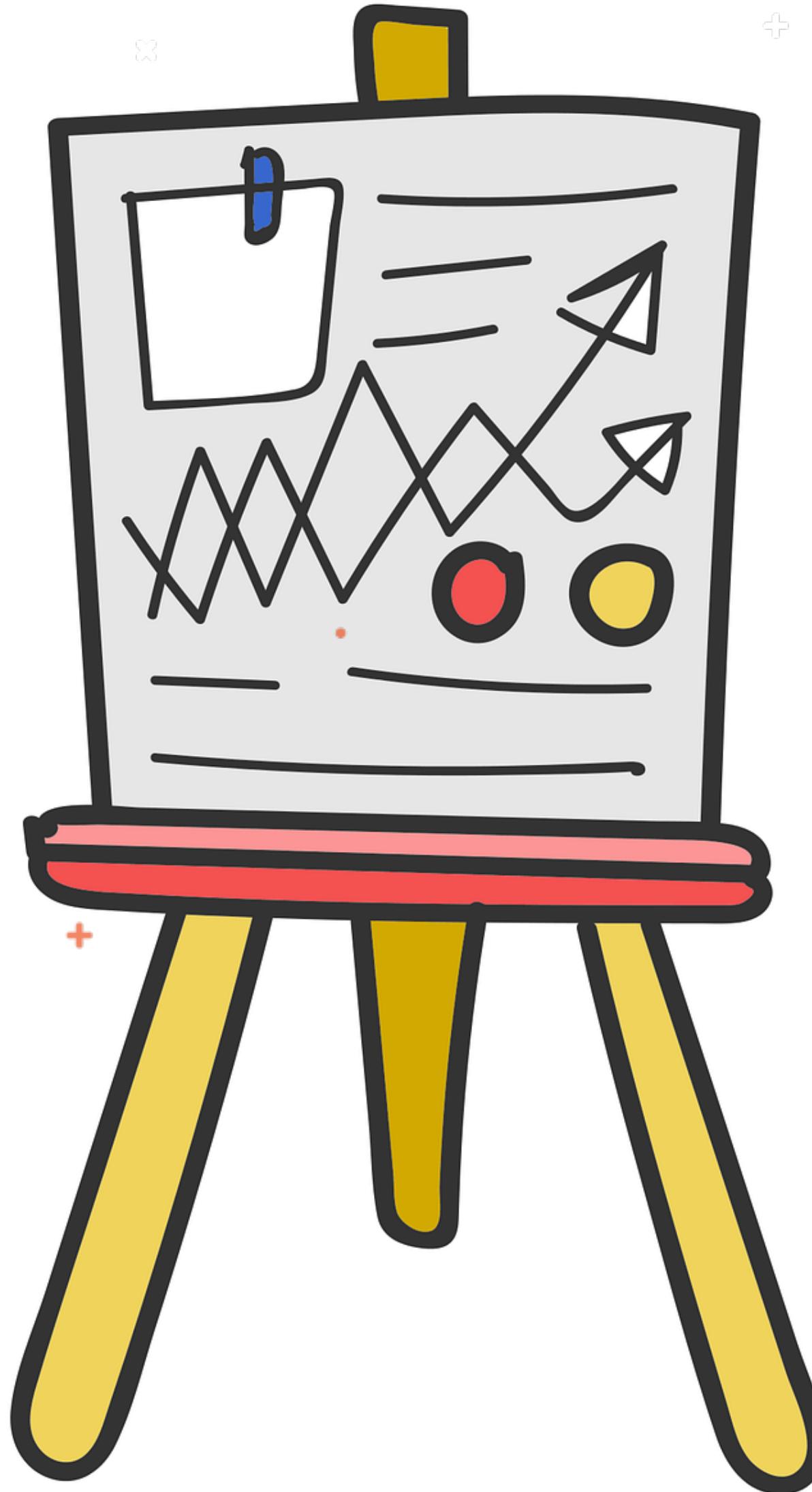




54%

Increase in data breaches in the first half of 2019 related to 2018.

@itrjwyss

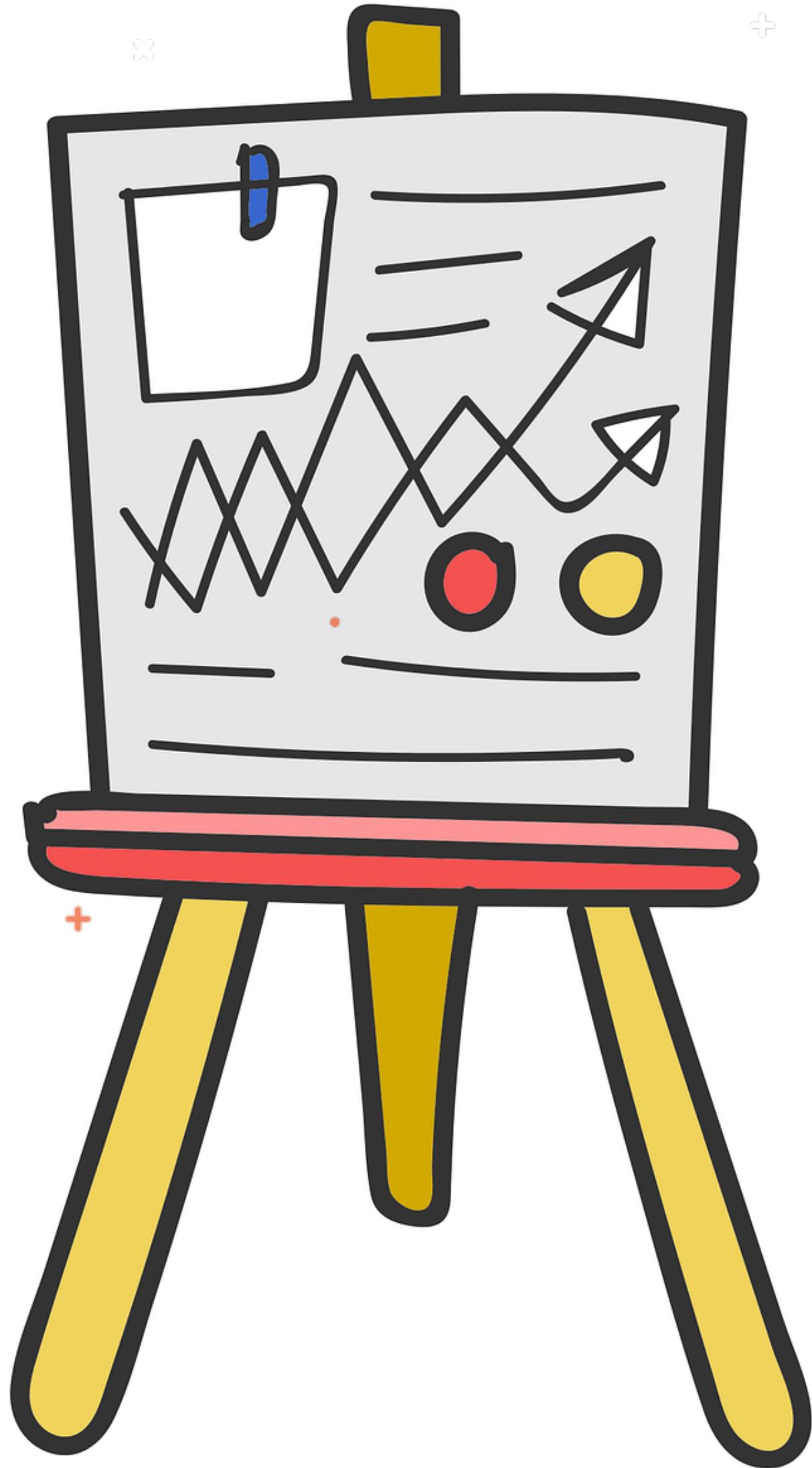


Oracle
Groundbreaker
Ambassador

3,800+

Data breaches were reported

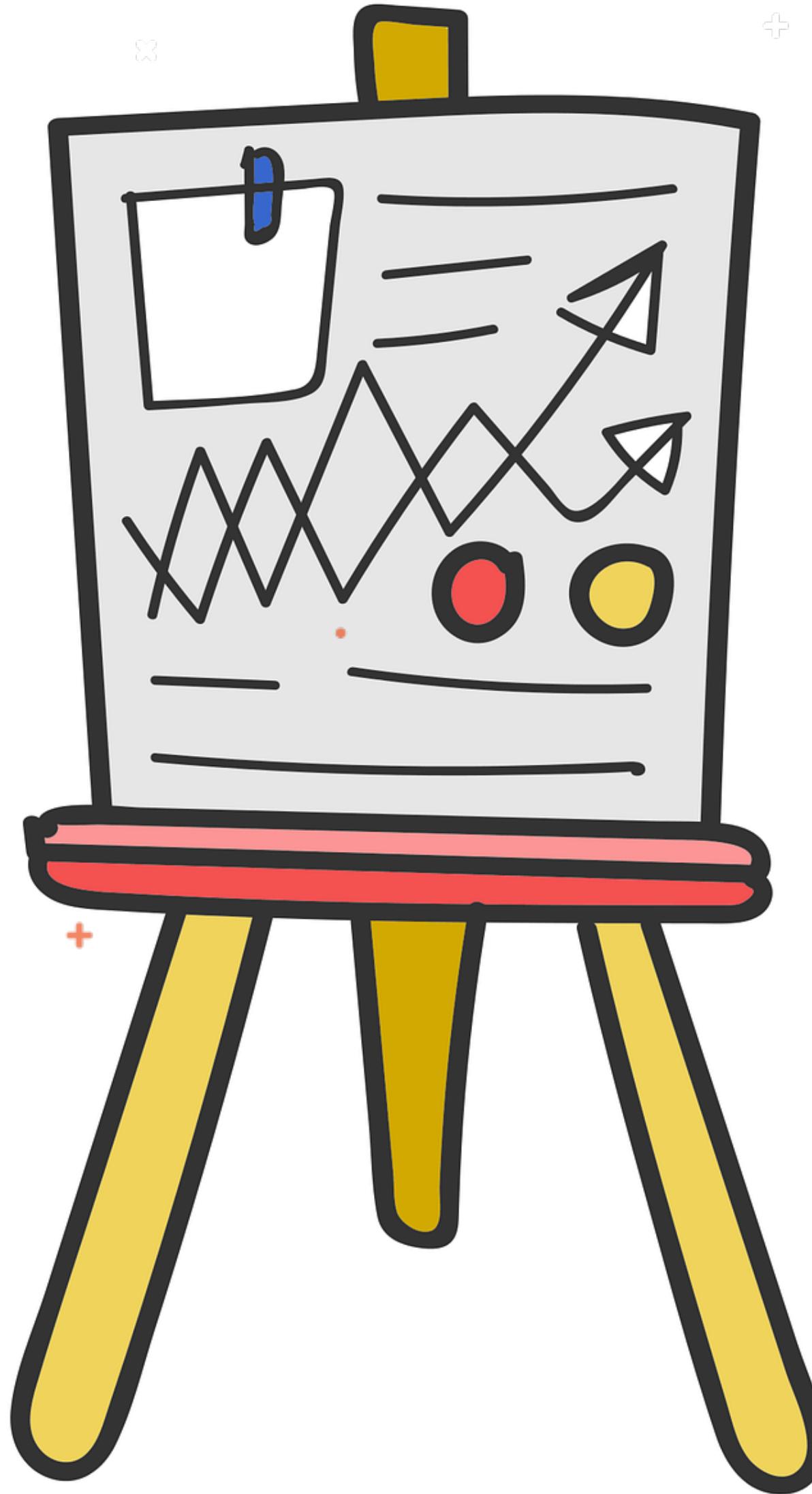
@itrjwyss



3.2 billion

Just eight of those

@itrjwyss



 Oracle
Groundbreaker
Ambassador

AMERICAN EQUIFAX



Had Been Uploaded



38,000
Driver's Licenses



3,200
Passport Details

@itrjwyss

 Oracle
Groundbreaker
Ambassador

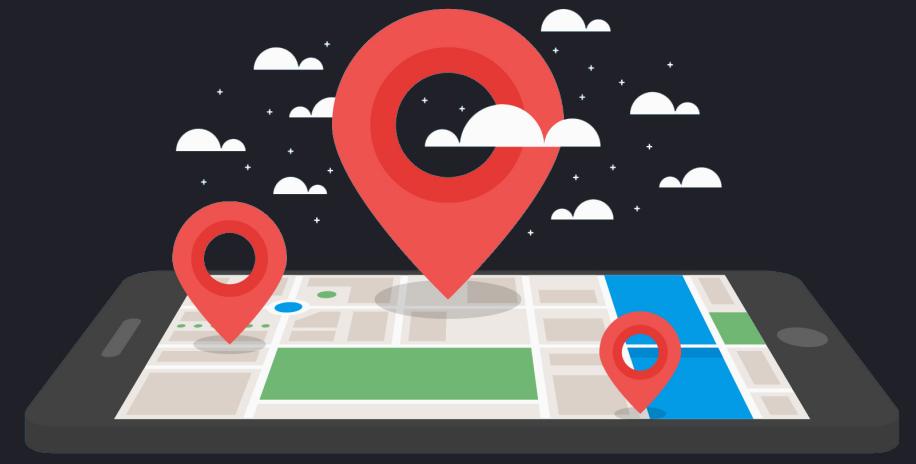
Had Stolen



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

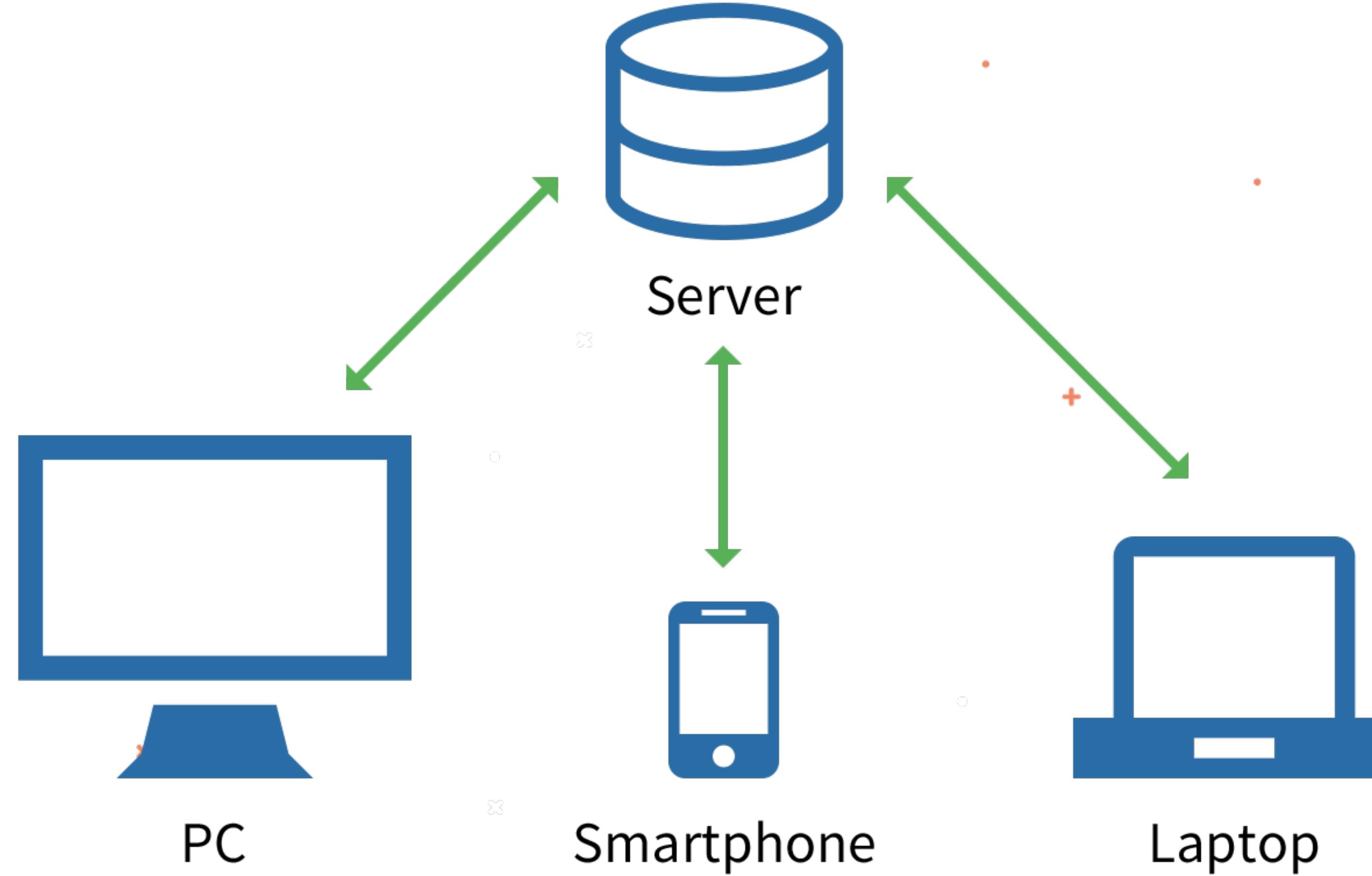


EU General Data
Protection Regulation
25 May 2018



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
- Identity as a Service (IDaaS)
- Architecture Level

@itrjwyss



Mercedes Wyss
@itrjwyss

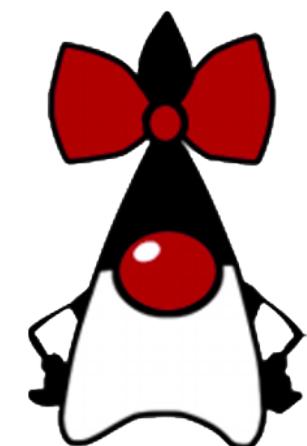


Oracle
Groundbreaker
Ambassador

⟨Devs⟩
+502

Comunidad Desarrolladores en Tecnologías
<Google> en Guatemala



JDuchess

Guatemala

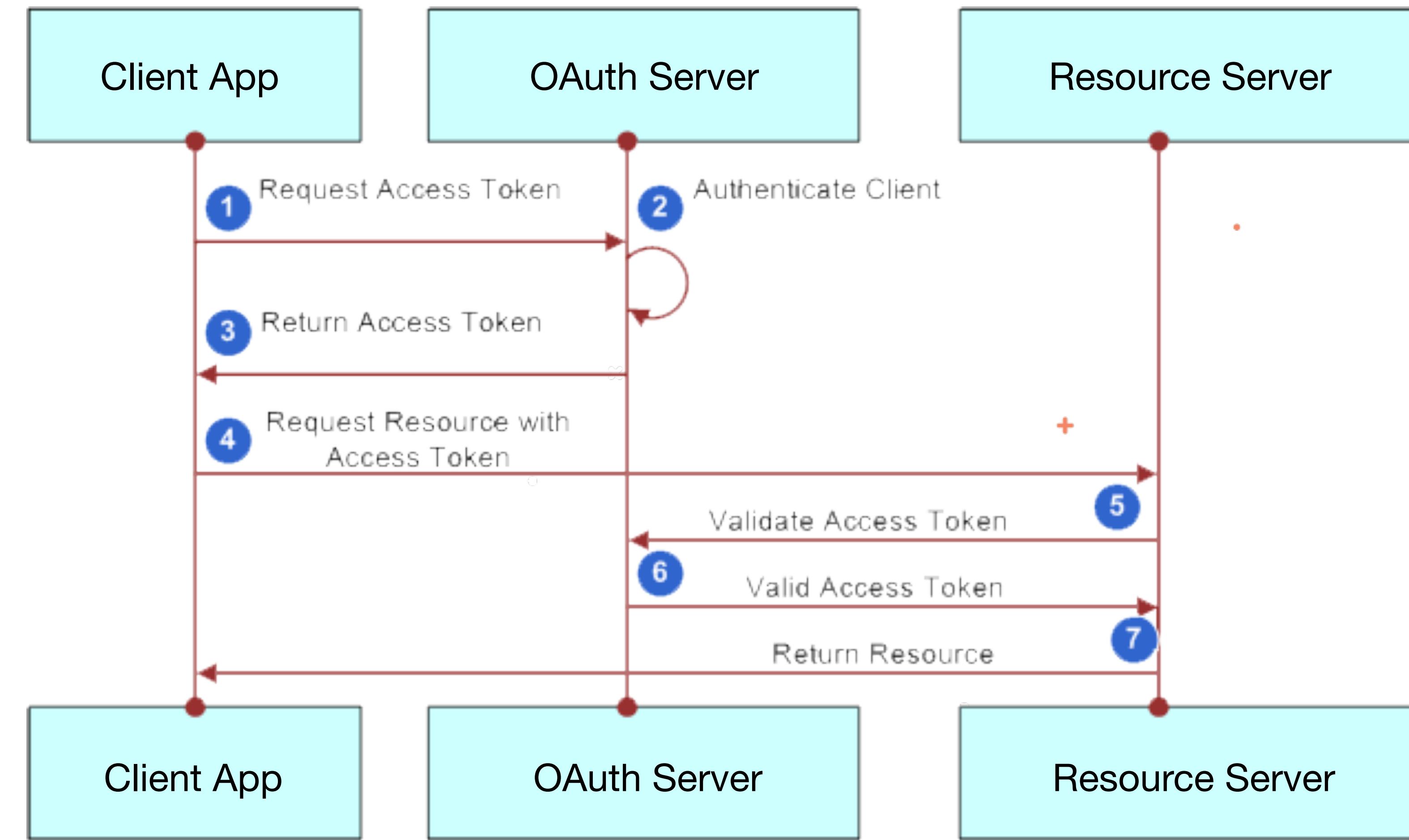
Bad API Design



@itrjwyss

 Oracle
Groundbreaker
Ambassador

OAuth



@itrjwyss

J

W

T



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

eyJhbGciOiJIUzI1NilsInR5cCI6IkpXVCJ
9eyJzdWliOilxMjM0NTY3ODkwliwibmF
tZSI6Ikpvag4gRG9IliwiYWRtaW4iOnRy
dWV9

Claims

@itrjwyss



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 |

@itrjwyss

Exploring JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCj9

- eyJqdGkiOiI1MWQ4NGFjMS1kYjMxLTRjM2It0TQw0S1lNjMwZWJiYj
gZZGYiLCJ1c2VybmtZSI6Imh1bnRlcjIiLCJzY29wZXMi0lsicmVw
bzpyZWFKIiwiZ2lzdDp3cm10ZSJdLCJpc3Mi0iIxNDUyMzQzMzcyIi
wiZXhwIjoiMTQ1MjM00TM3MiJ9

- cS5KkPxtEJ9eonvsGvJBZFIamDnJA7gSz3HZBWv6S1Q

Exploring JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCj9 **Header**
▪
eyJqdGkiOiI1MWQ4NGFjMS1kYjMxLTRjM2It0TQwOS1lNjMwZWJiYj
gZZGYiLCJ1c2VybmtZSI6Imh1bnRlcjIiLCJzY29wZXMiOlsicmVw
bzpyZWFKIiwiZ2lzdDp3cm10ZSJdLCJpc3Mi0iIxNDUyMzQzMzcyIi
wiZXhwIjoiMTQ1MjM00TM3MiJ9 **Claims**
▪
cS5KkPxtEJ9eonvsGvJBZFIamDnJA7gSz3HZBWv6S1Q **Signature**

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

@itrjwyss



Oracle
Groundbreaker
Ambassador

What problems does JWT solve?

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

@itrjwyss



Oracle
Groundbreaker
Ambassador

Client

Server

1. POST /users/login with username and password

3. Returns the JWT to the Browser

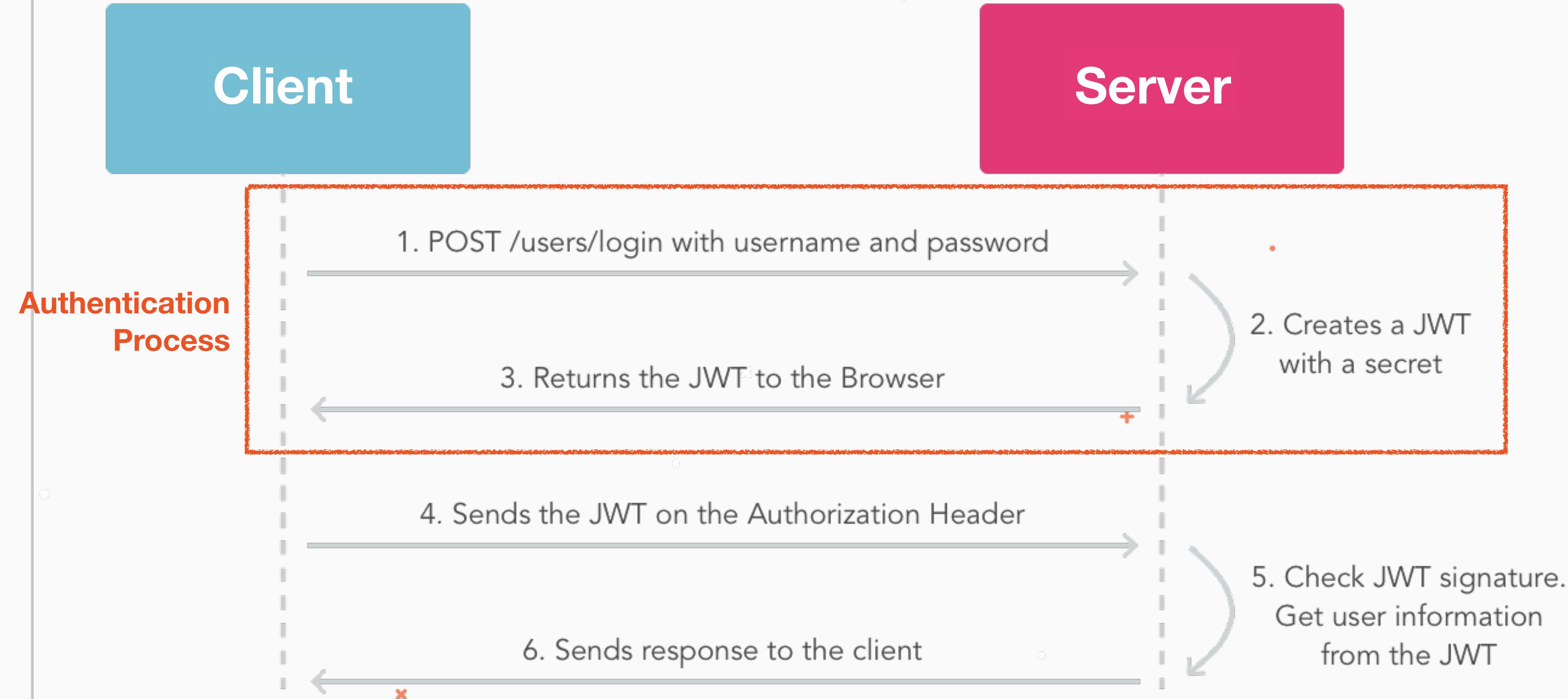
4. Sends the JWT on the Authorization Header

6. Sends response to the client

2. Creates a JWT with a secret

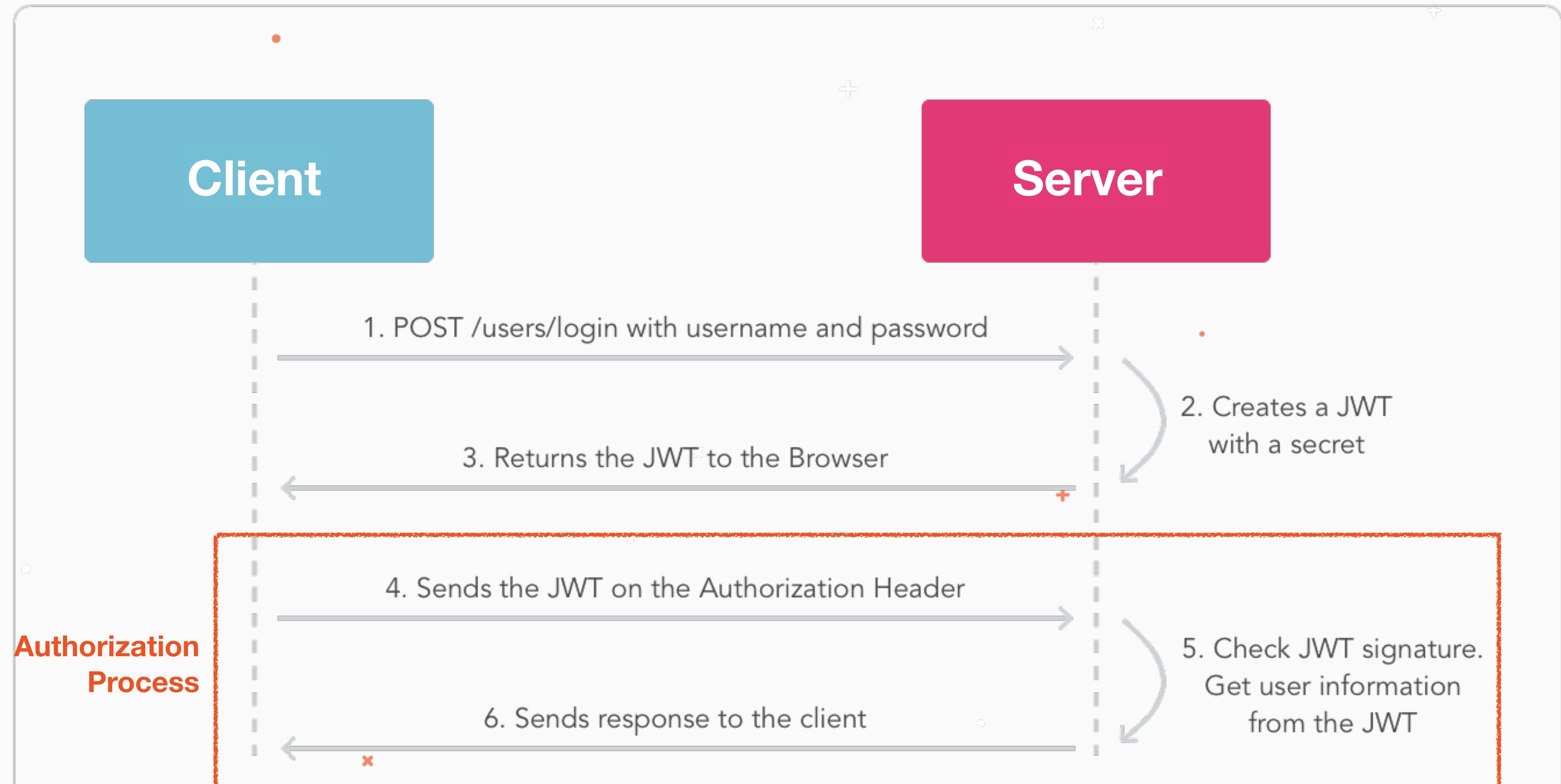
5. Check JWT signature.
Get user information from the JWT

@itrjwyss



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





@itrjwyss

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





[Debugger](#) [Libraries](#) [Introduction](#) [Ask](#) [Get a T-shirt!](#)

Crafted by Auth0

Debugger

ALGORITHM

HS256

Encoded

PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdI
Ii0iIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9I:
iwiYWRtaW4iOnRydWV9.TJVA950rM7E2cBab30RMHrI
DcEfjoYZgeF0NFh7HgQ

Decoded

EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

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



Oracle Groundbreaker Ambassador



@itrjwyss



• Improve API Design



@itrjwyss

 Oracle
Groundbreaker
Ambassador

User Credentials Problem



Username : admin
Password : admin

@itrjwyss





SSO

Single Sign On

@itrjwyss

 Oracle
Groundbreaker
Ambassador

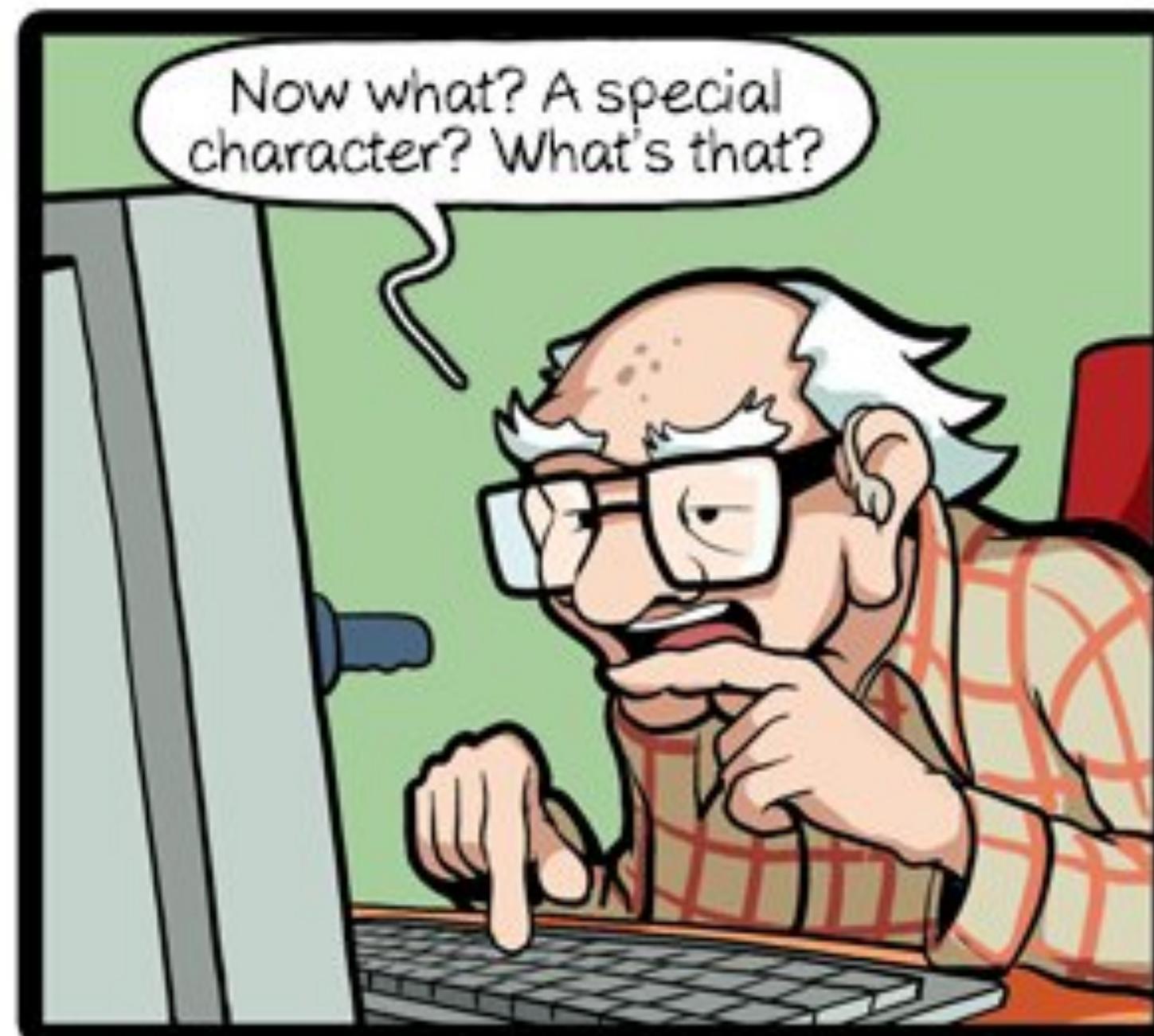
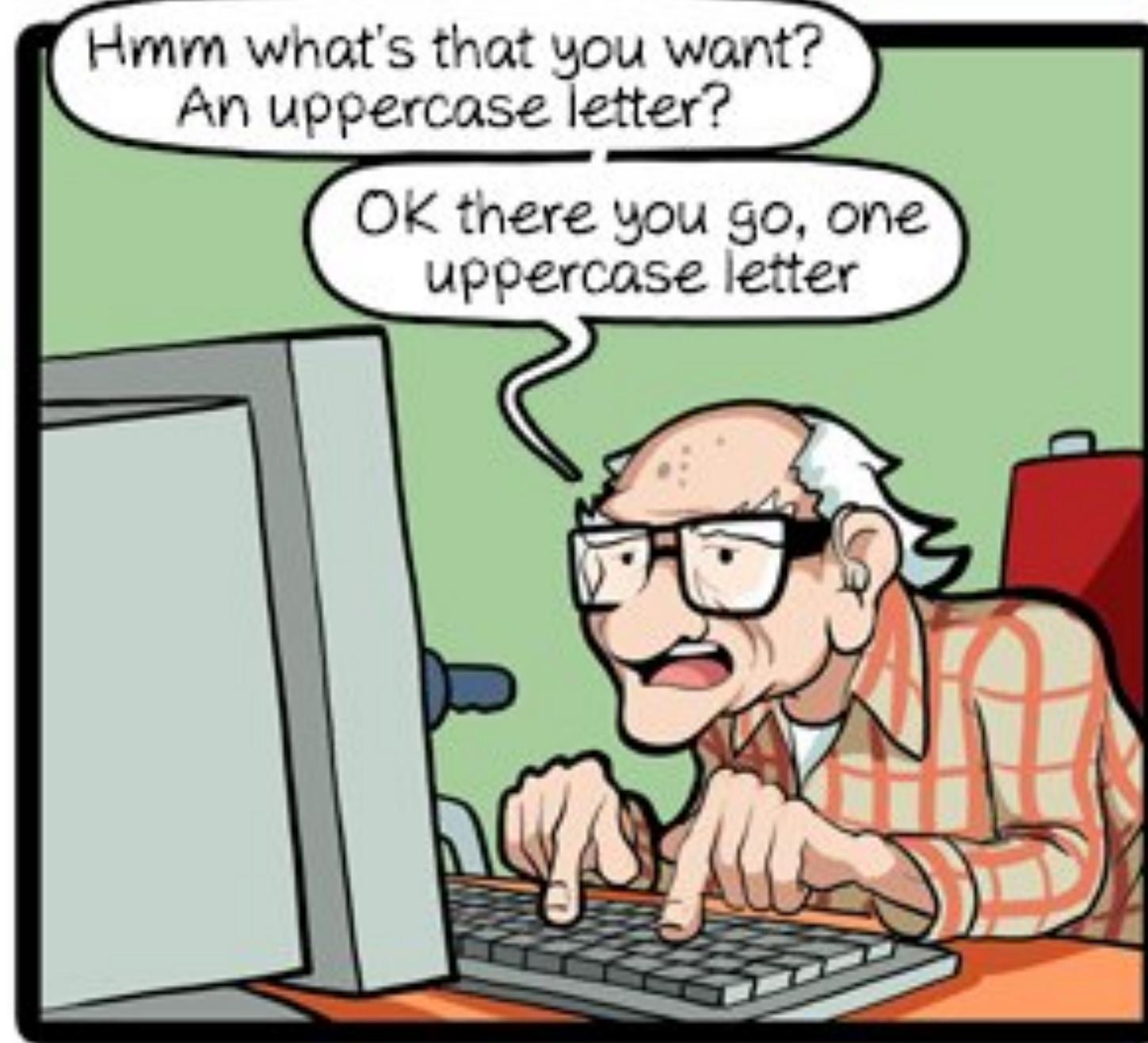


PASSWORD

IRULES!

@itrjwyss





@itrjwyss



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



Oracle
Groundbreaker
Ambassador





CHARLOTTE



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

@itrjwyss



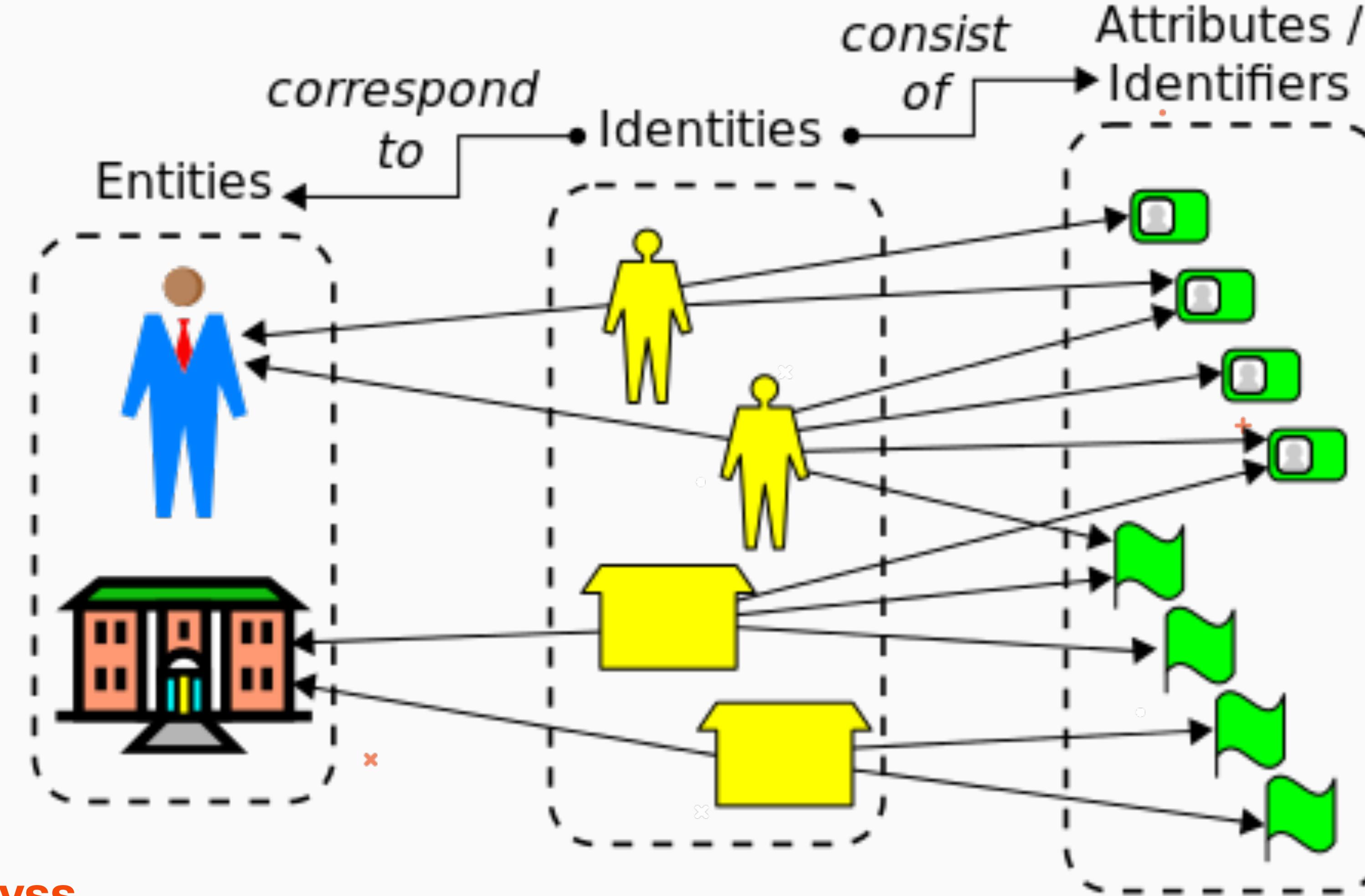
Identity Management (IdM)

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

@itrjwyss



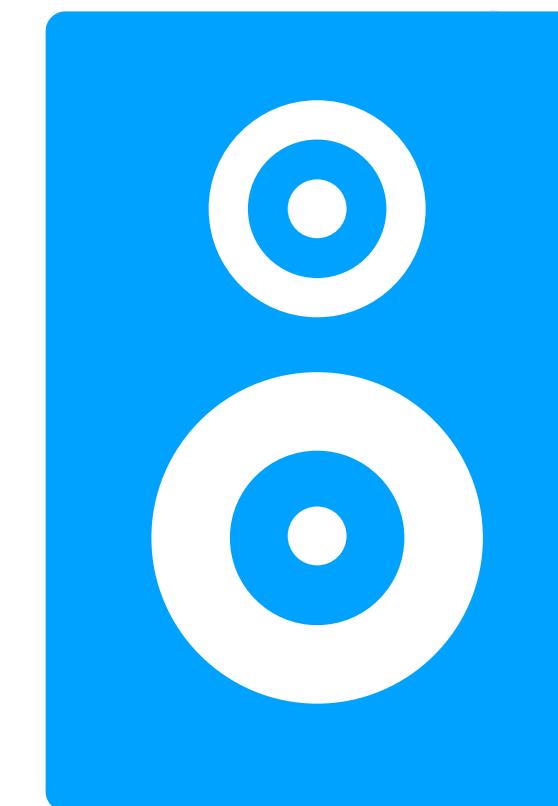
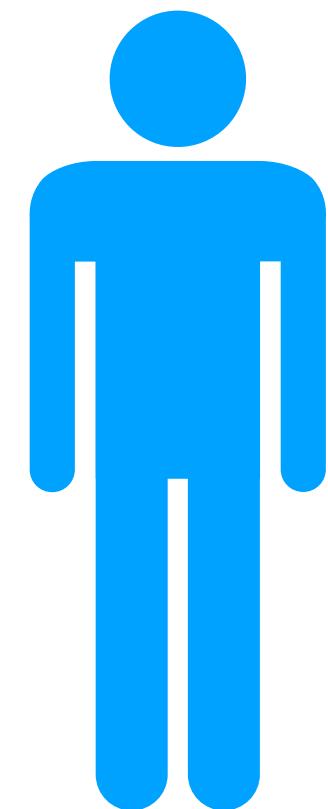
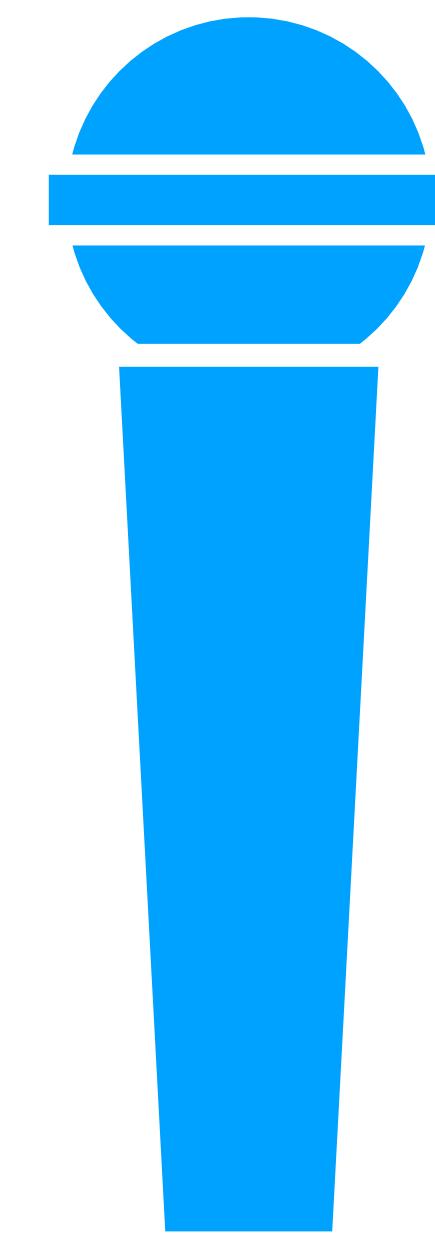
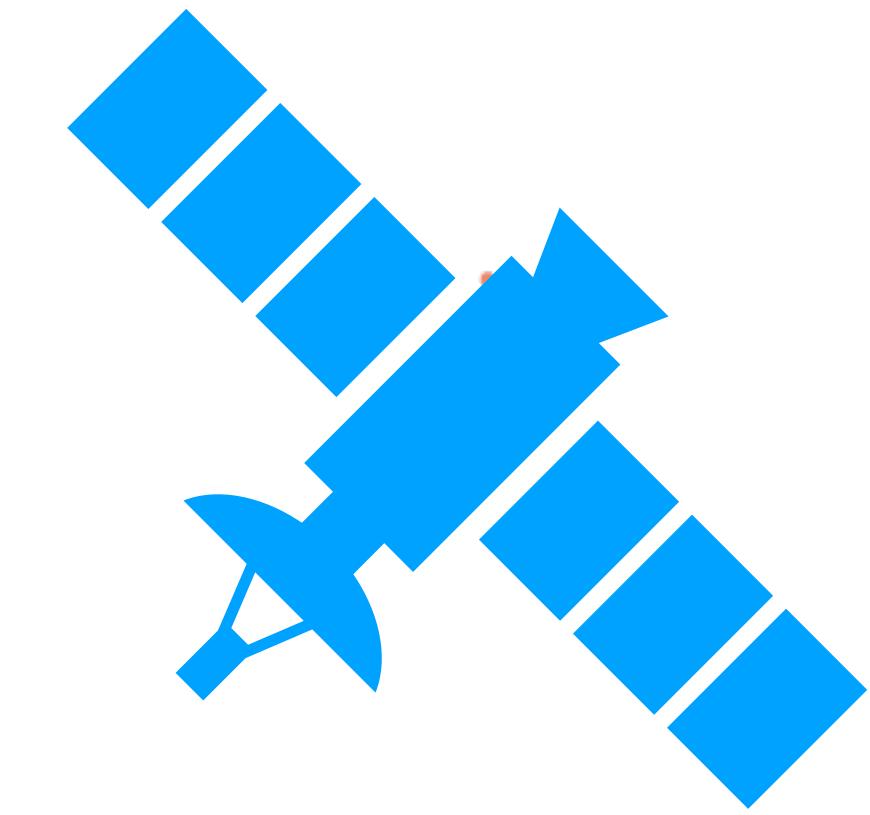
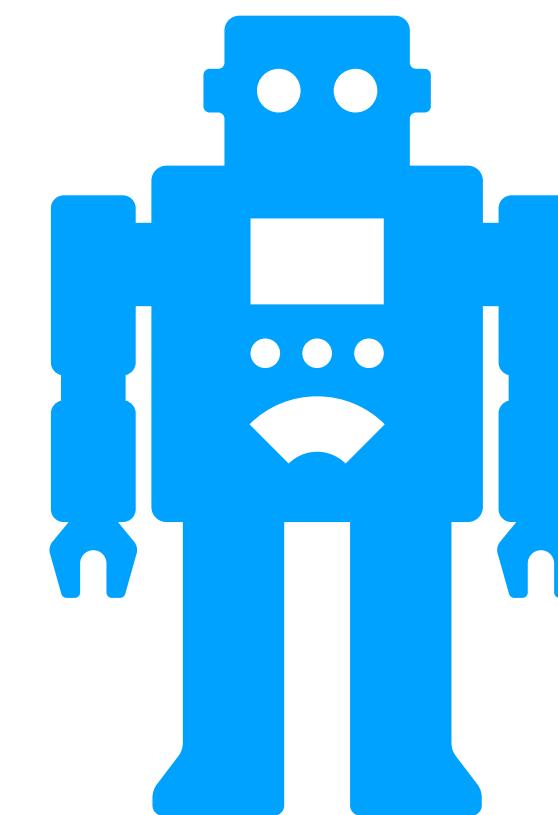
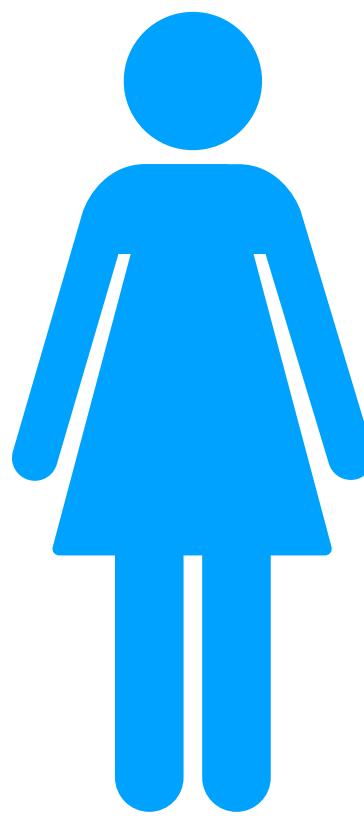
IdM: Provisioning



@itrjwyss

Oracle
Groundbreaker
Ambassador

IdM: Provisioning



@itrjwyss



IdM: Account Management

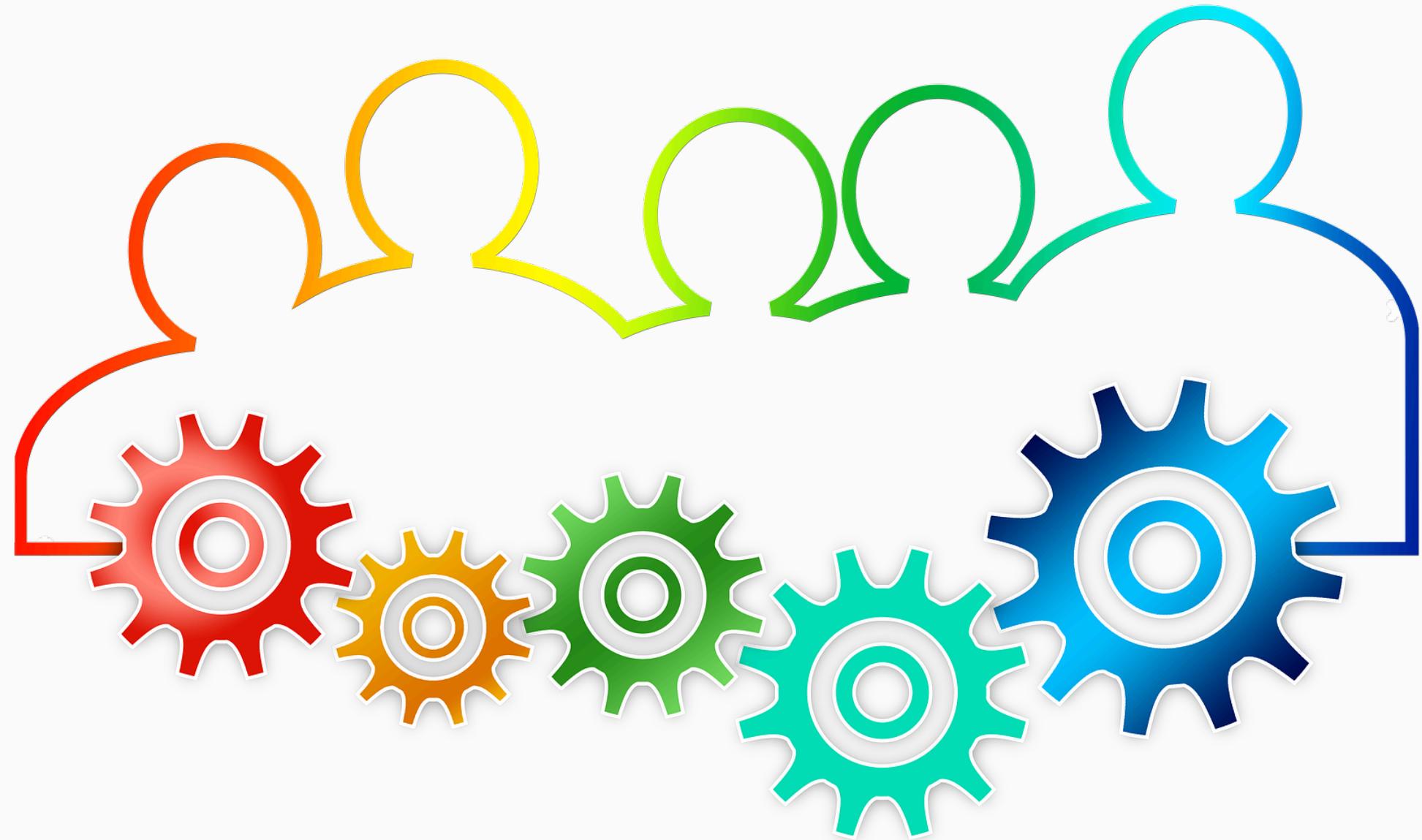
- Maintain those identities
- How safe those data?
- Encryption, Which one, which keys?
- What happens when an Entity erase their account?
- What happens when an Entity is longer inactive?

@itrjwyss



IdM: Identity Governance

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



Identity and Access Management (IAM)

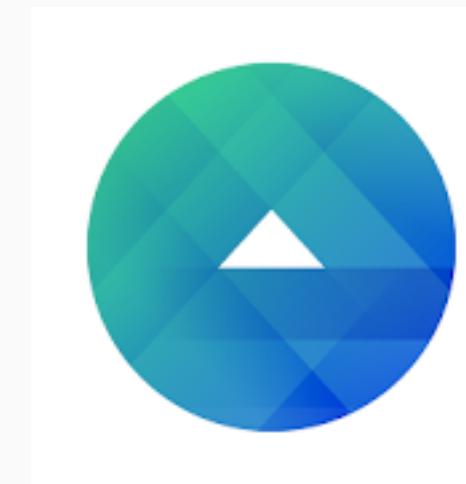
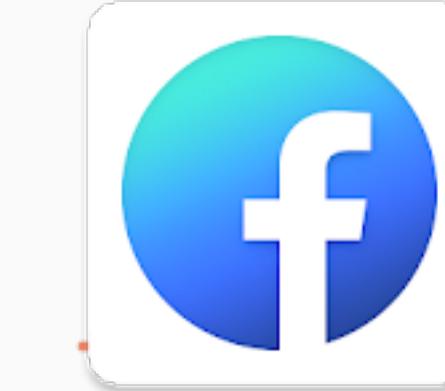
- Is most often used to refer not just to identification, but to the whole suite of practices that a corporation needs to manage their users and data:
 - Authentication
 - Authorization
 - Identity Federation

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.

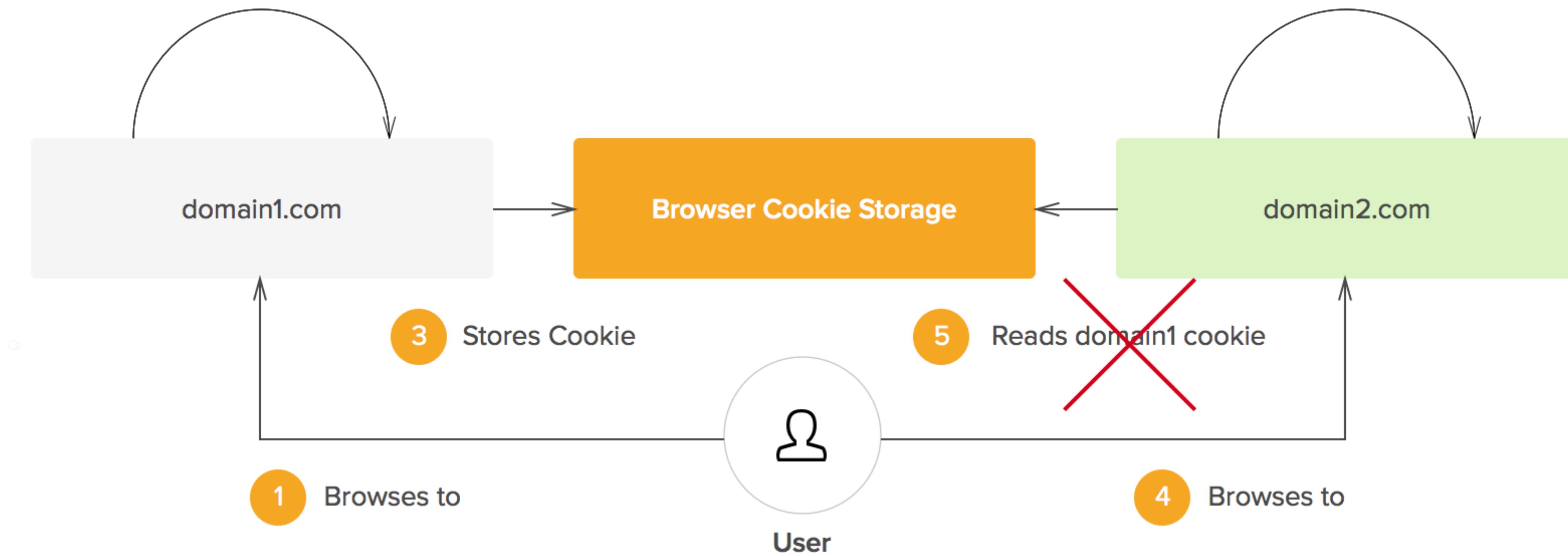


@itrjwyss

Oracle
Groundbreaker
Ambassador

SAME-ORIGIN-POLICY FORBIDS THIS

- 2 Ask for login info, authenticates user
- 6 Uses cookie domain1, authenticates user

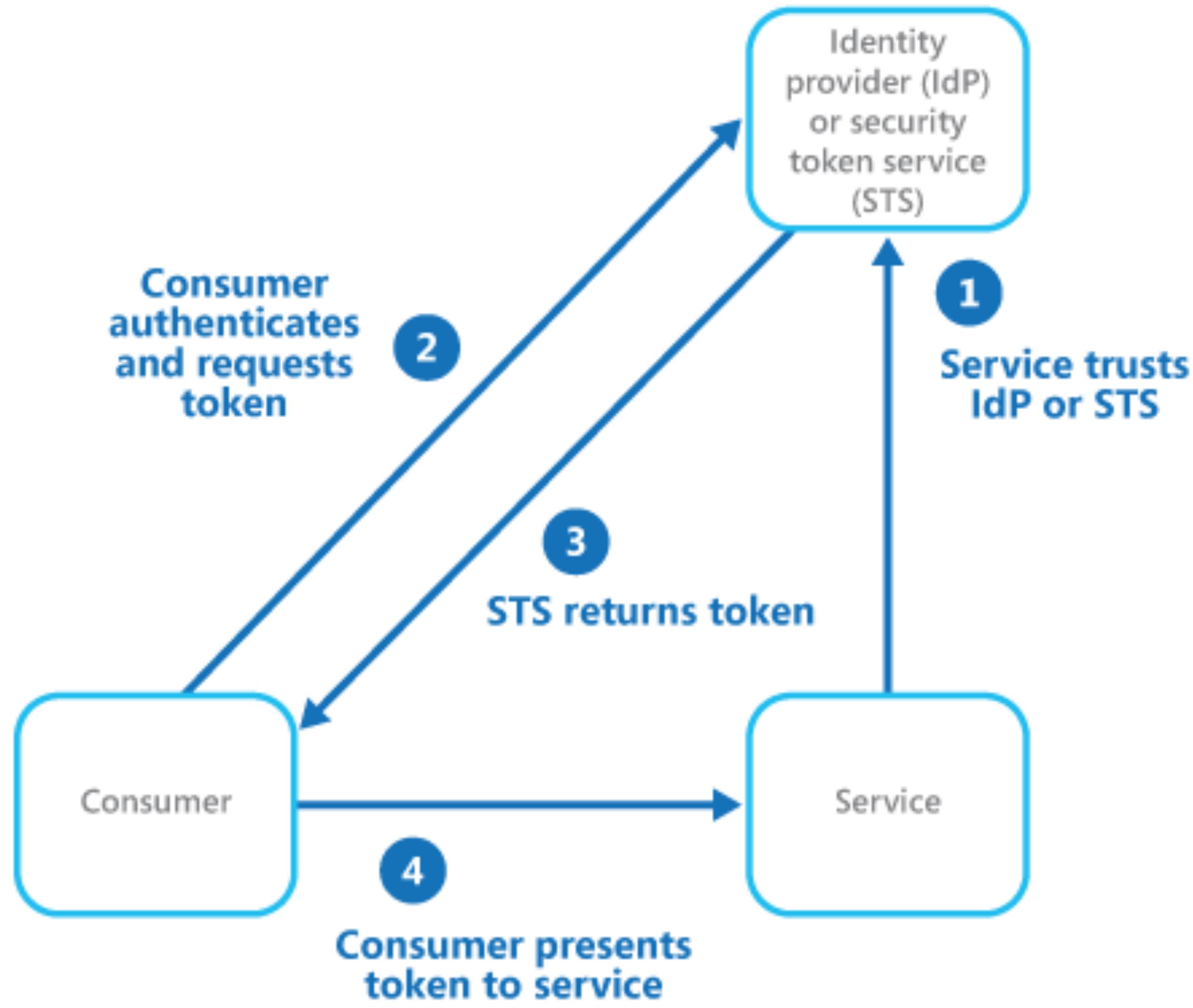


Federated Identity

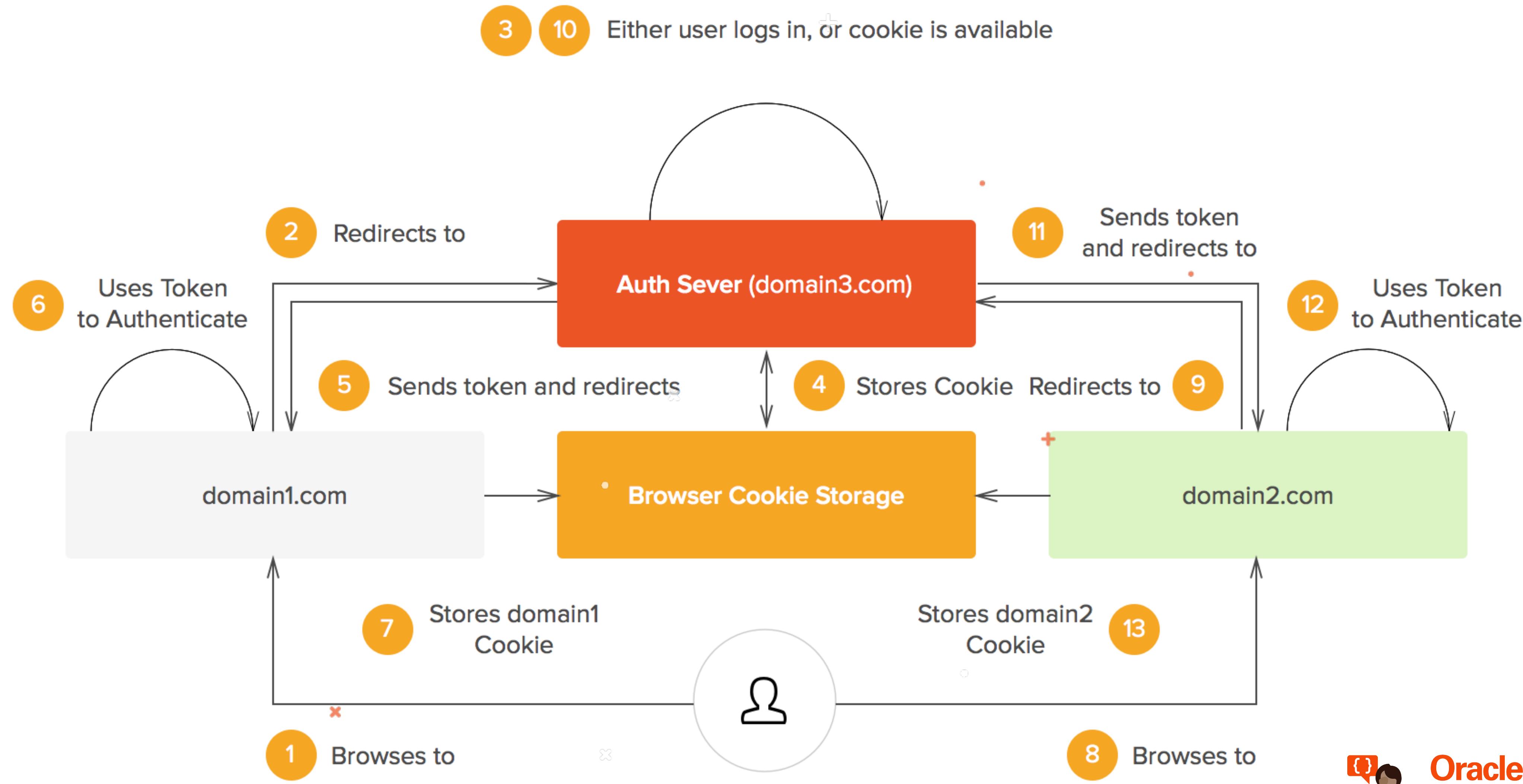
- In some way, are methods of transferring data without violating the same origin policy.
- This way, if domain X and Y are related, and their⁺owners want users to move freely between the two, they can simply triangulate around an external authorization server.

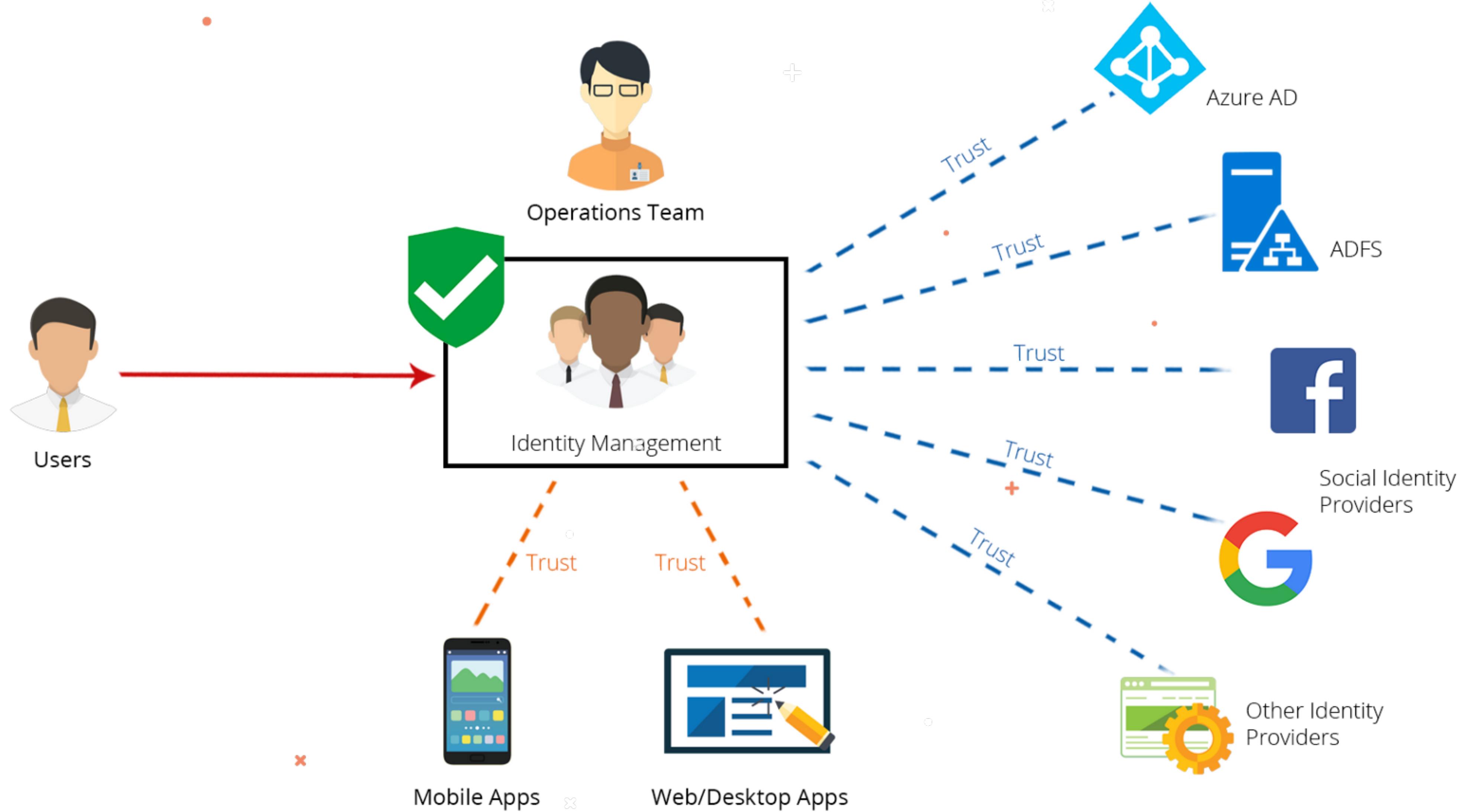
@itrjwyss





TYPICAL SSO





@itrjwyss



IAM: Authentication

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

@itrjwyss



IAM: Authentication

- Ensuring that a given user is the user they identify as

- Single Sing On (SSO)

- Multi-factor Authentication (MFA)

- Passwordless



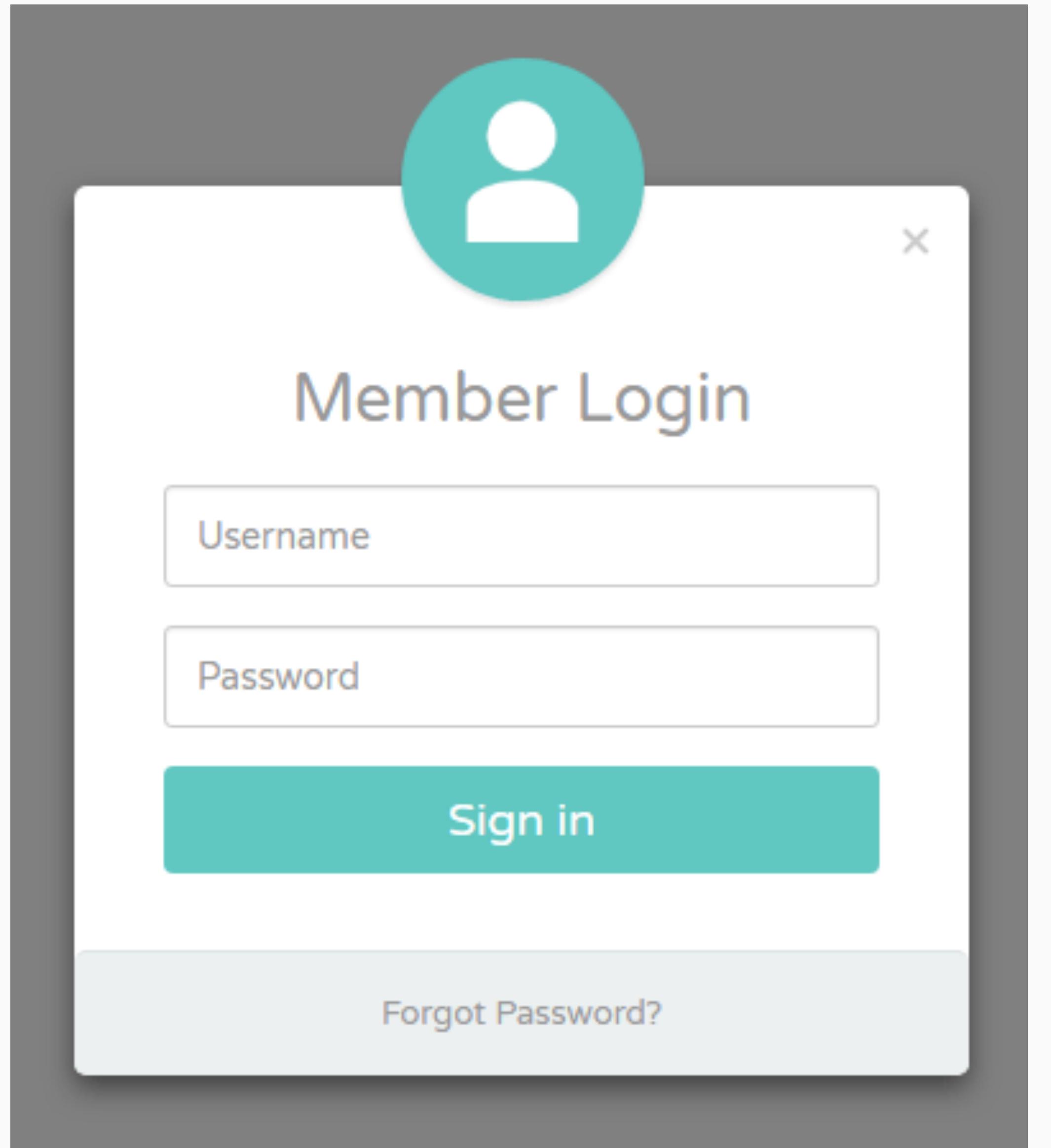
Knowledge



Possession



Biometric



A screenshot of a Member Login interface. At the top is a teal circular icon containing a white user silhouette. Below it is the title "Member Login". There are two input fields: "Username" and "Password", both with placeholder text. A large teal "Sign in" button is centered below the inputs. At the bottom is a light gray bar with the text "Forgot Password?".

Member Login

Username

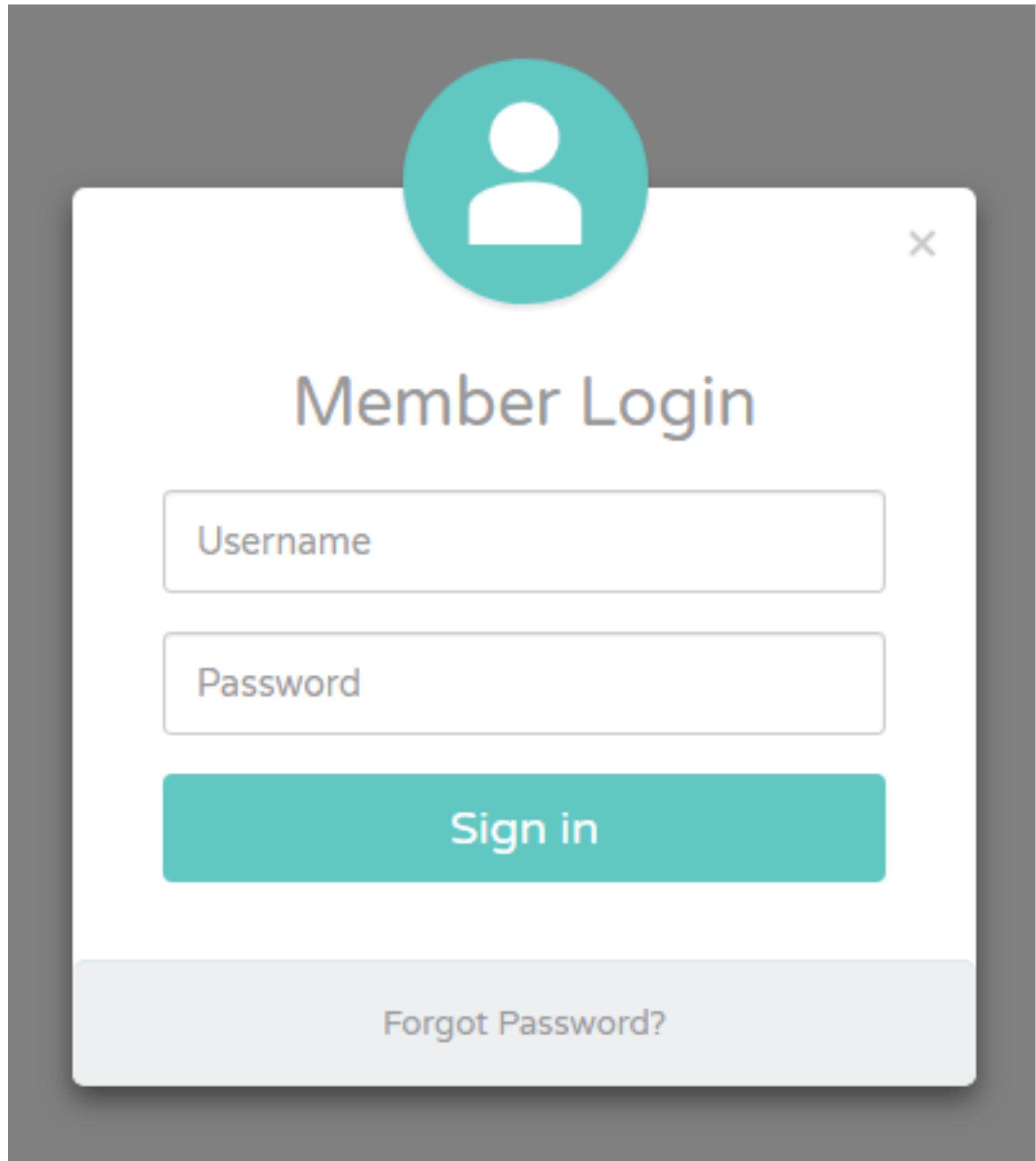
Password

Sign in

Forgot Password?

@itrjwyss





A screenshot of a member login interface. At the top is a teal circular icon containing a white user silhouette. To its right is a small gray 'X' button. Below the icon is the text "Member Login". The main area contains two input fields: "Username" and "Password", both with placeholder text. Below these is a large teal "Sign in" button. At the bottom is a light gray bar with the text "Forgot Password?".

Member Login

Username

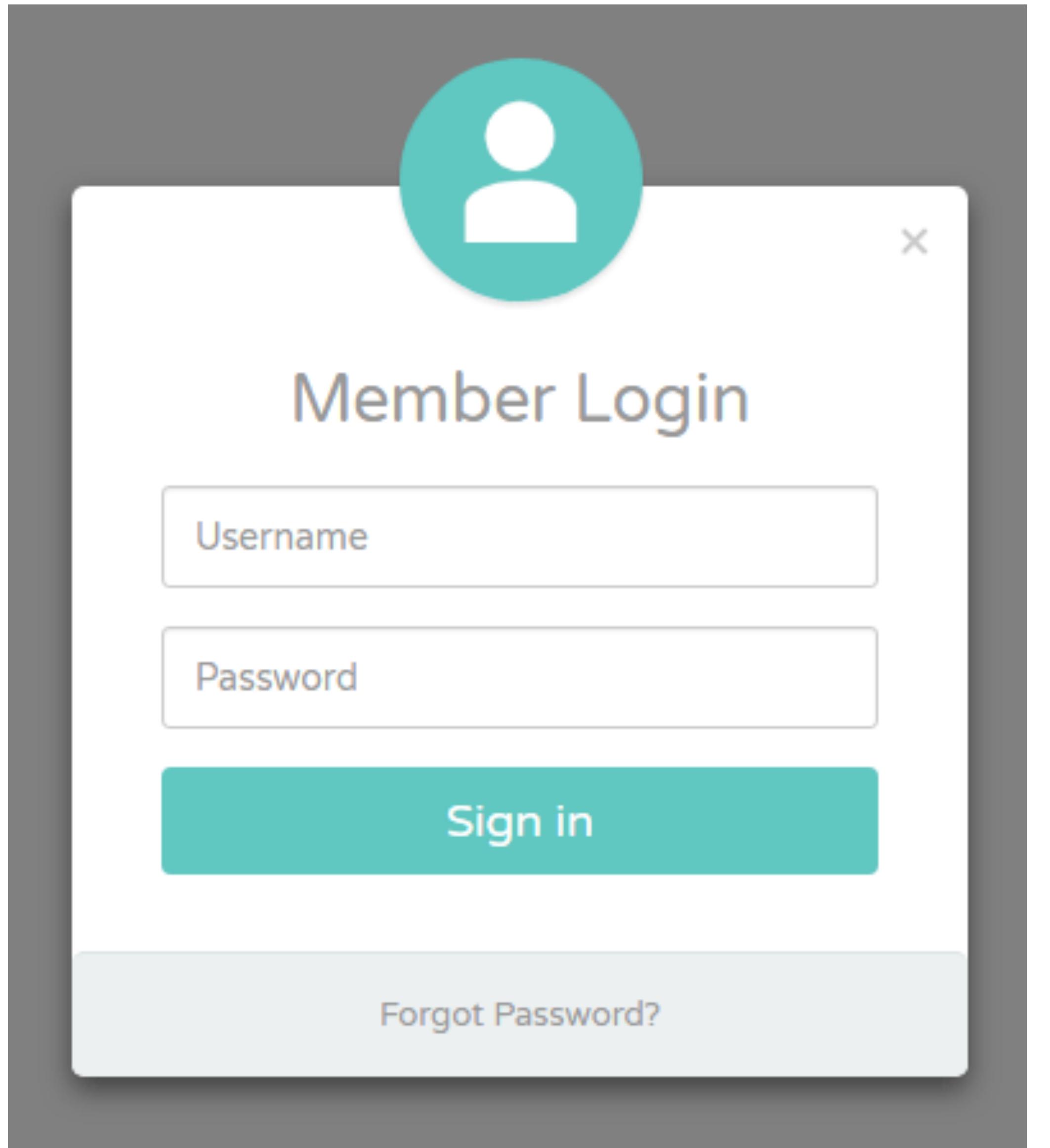
Password

Sign in

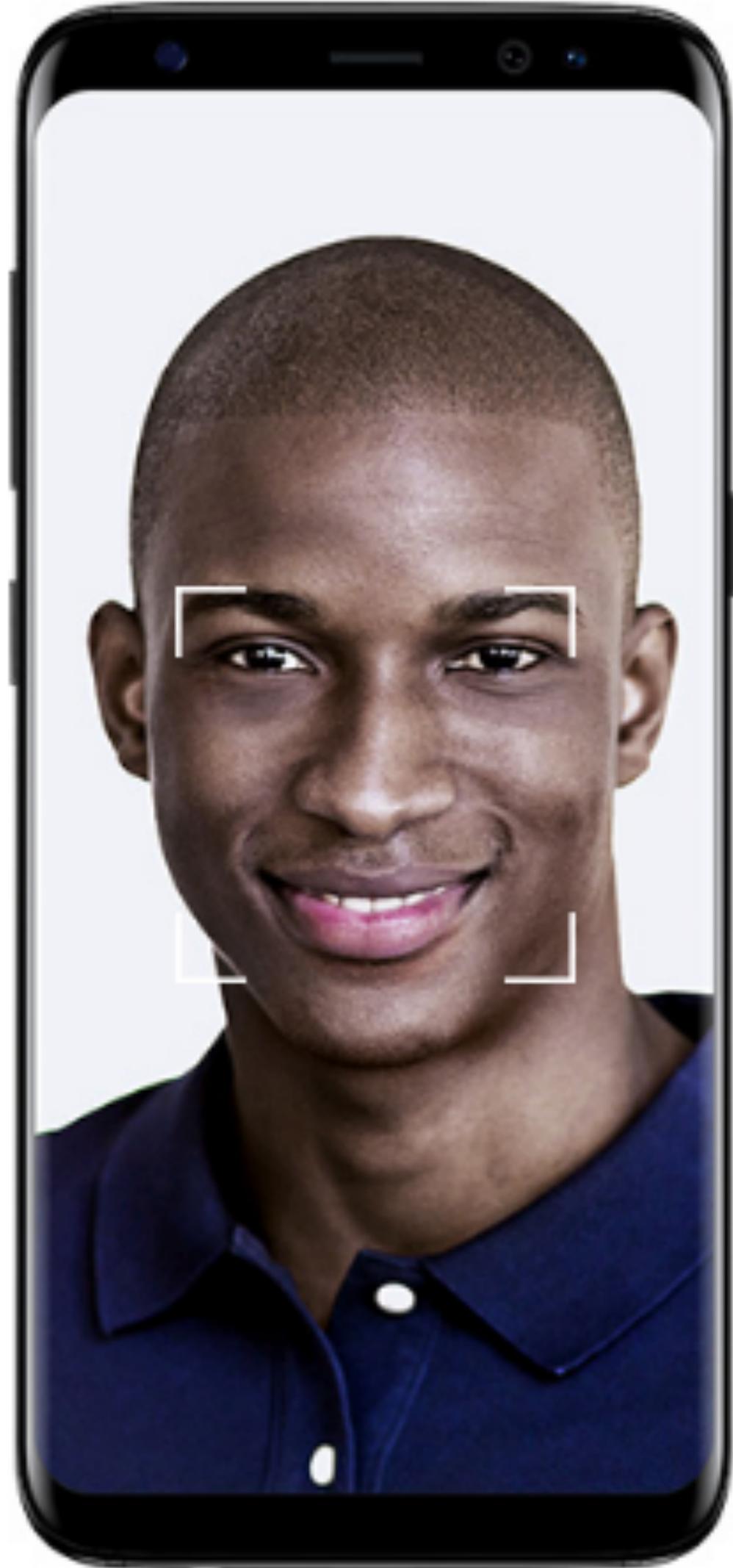
Forgot Password?



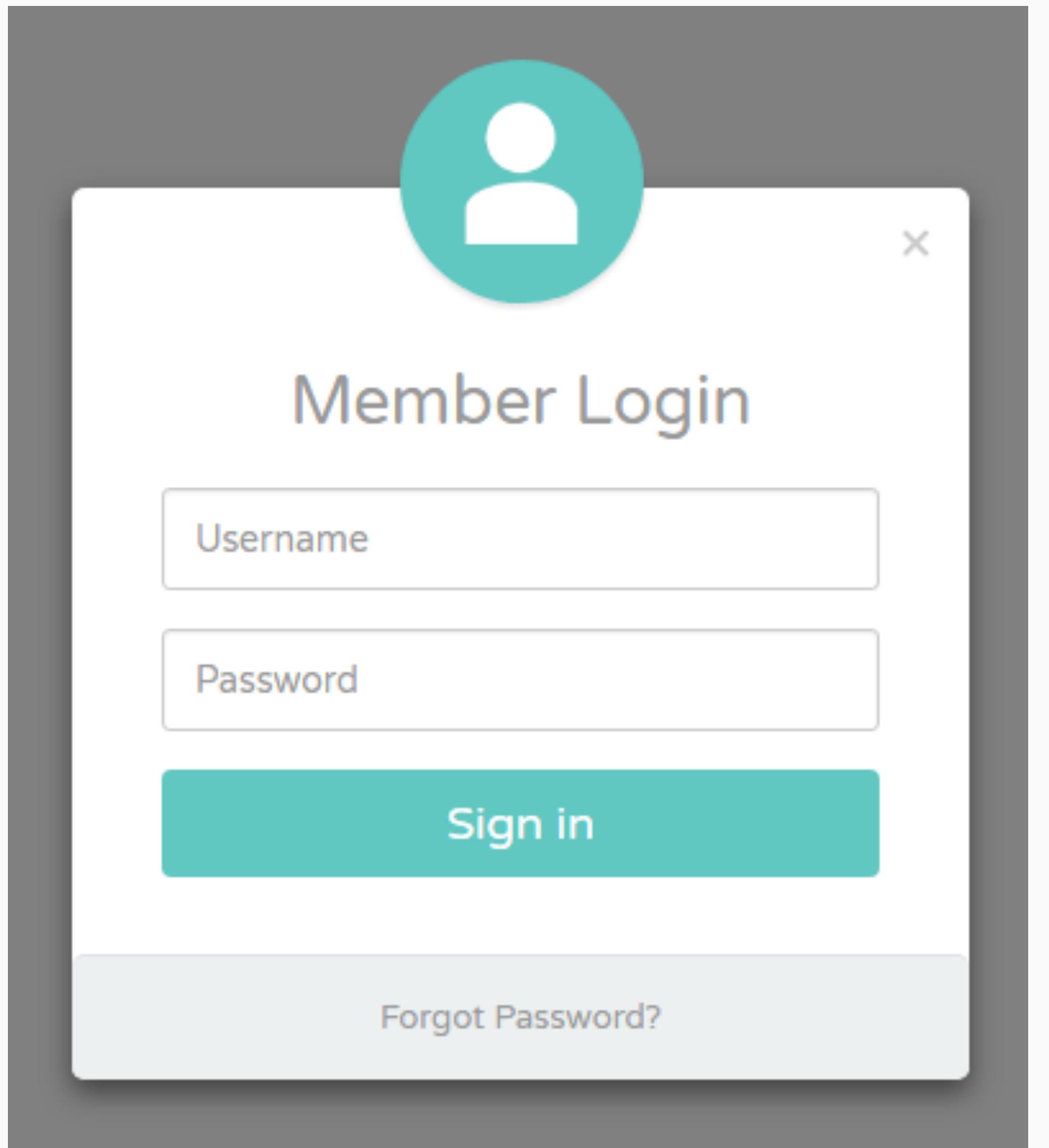
@itrjwyss



@itrjwyss



Oracle
Groundbreaker
Ambassador



A screenshot of a Member Login interface. At the top is a teal circular icon containing a white user silhouette. Below it, the text "Member Login" is displayed in a dark blue font. The form contains two input fields: "Username" and "Password", both with placeholder text. A large teal "Sign in" button is centered below the inputs. At the bottom of the form is a link labeled "Forgot Password?".

@itrjwyss



Oracle
Groundbreaker
Ambassador



MFA

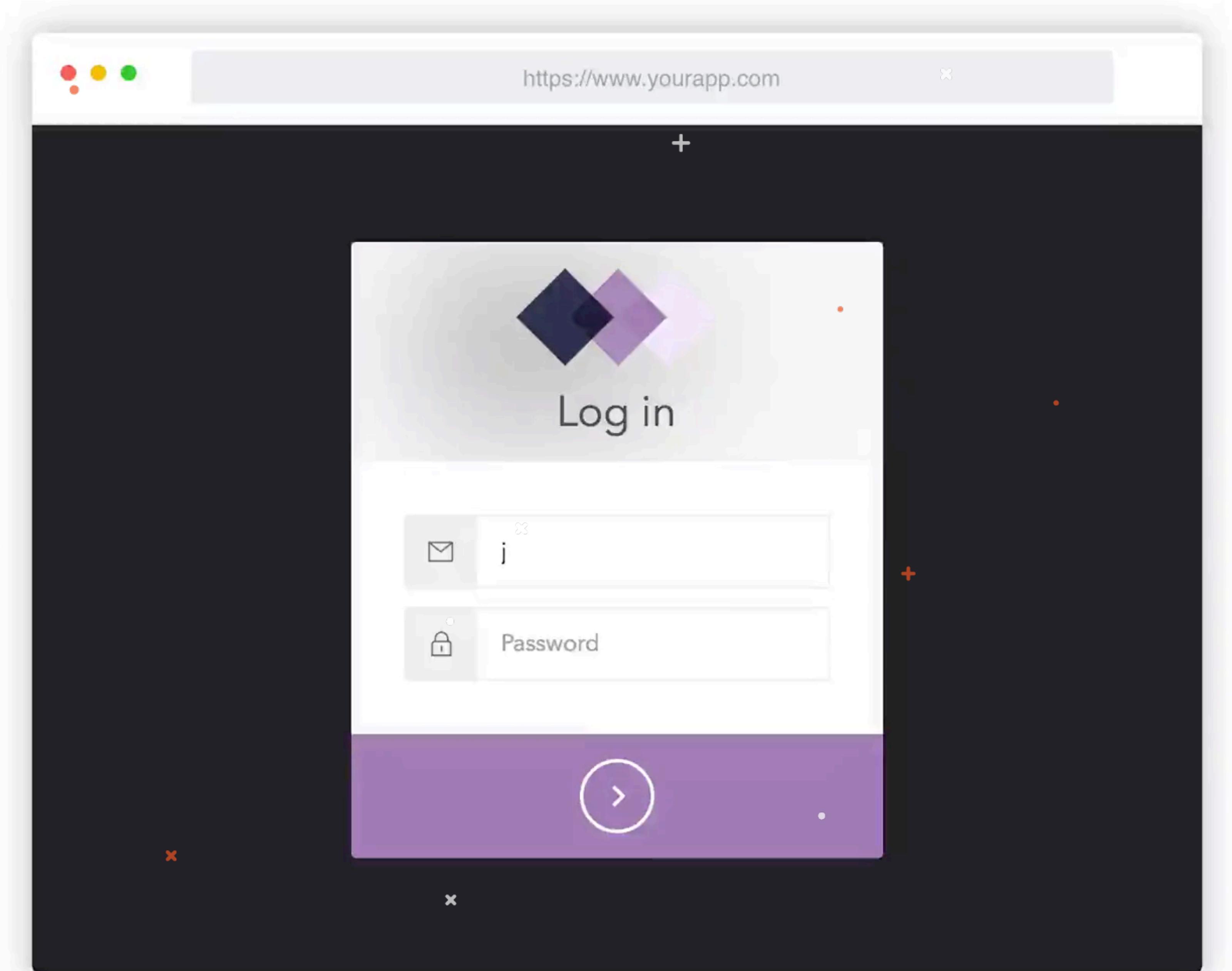
Multi-Factor
Authentication

@itrjwyss





@itrjwyss



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

@itrjwyss

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



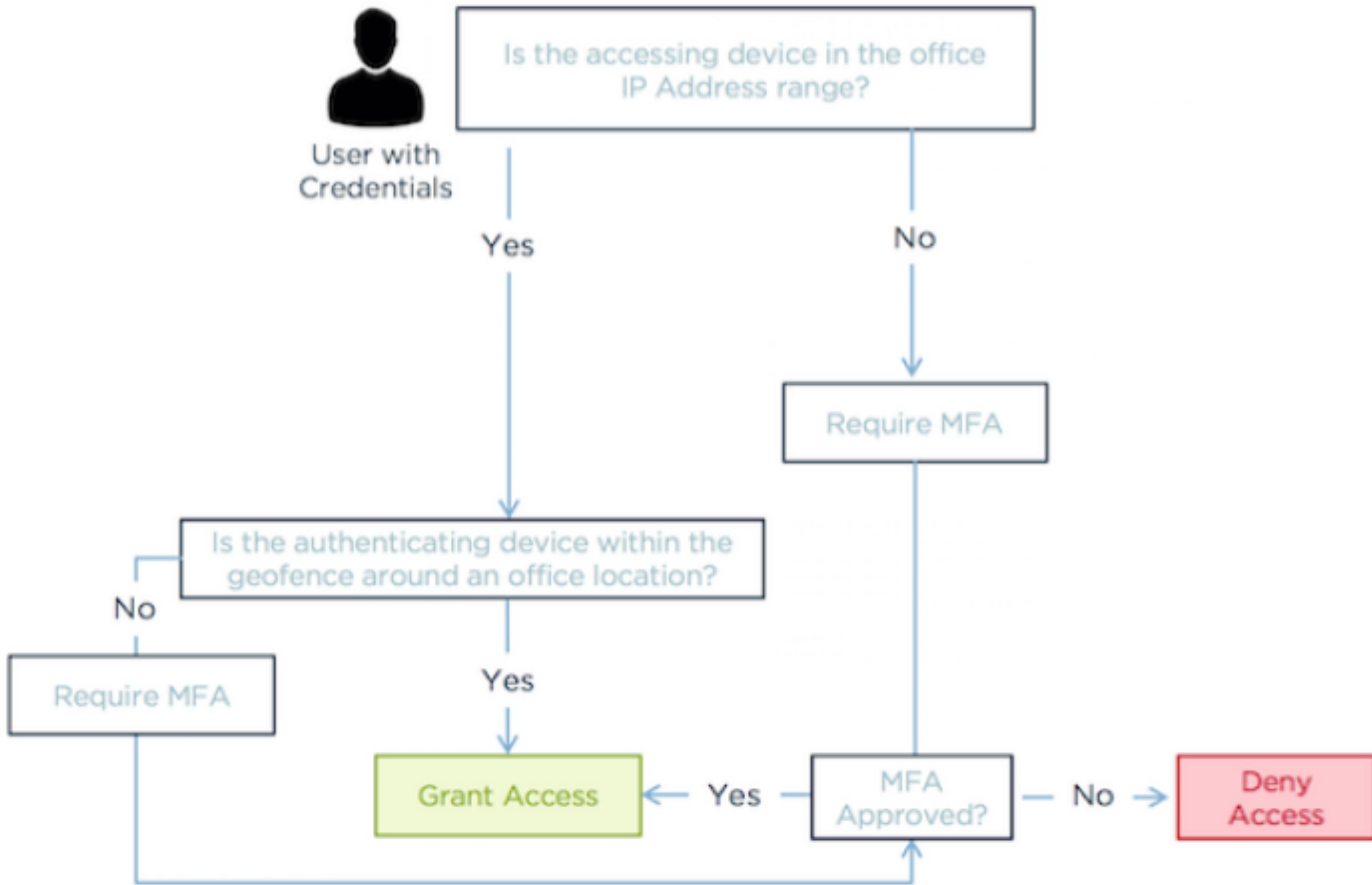
@itrjwyss

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.

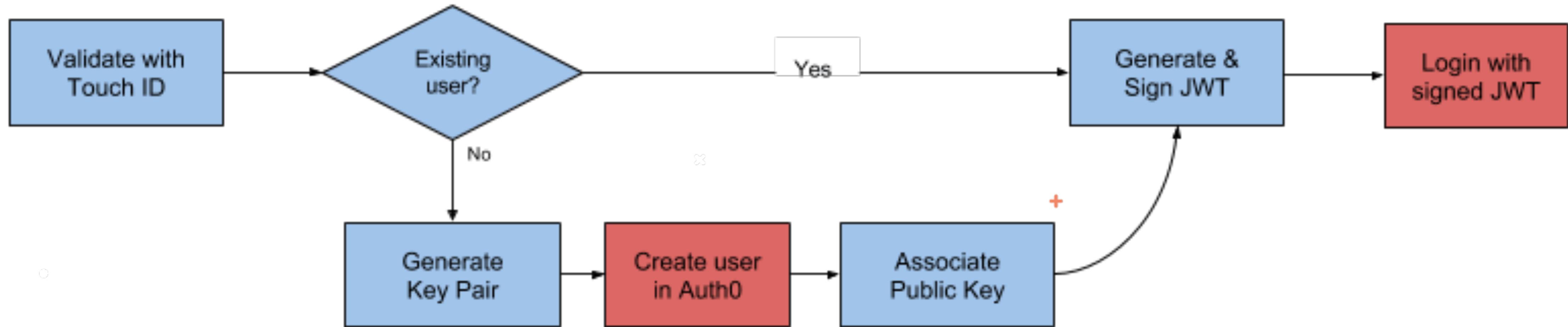
@itrjwyss





@itrjwyss

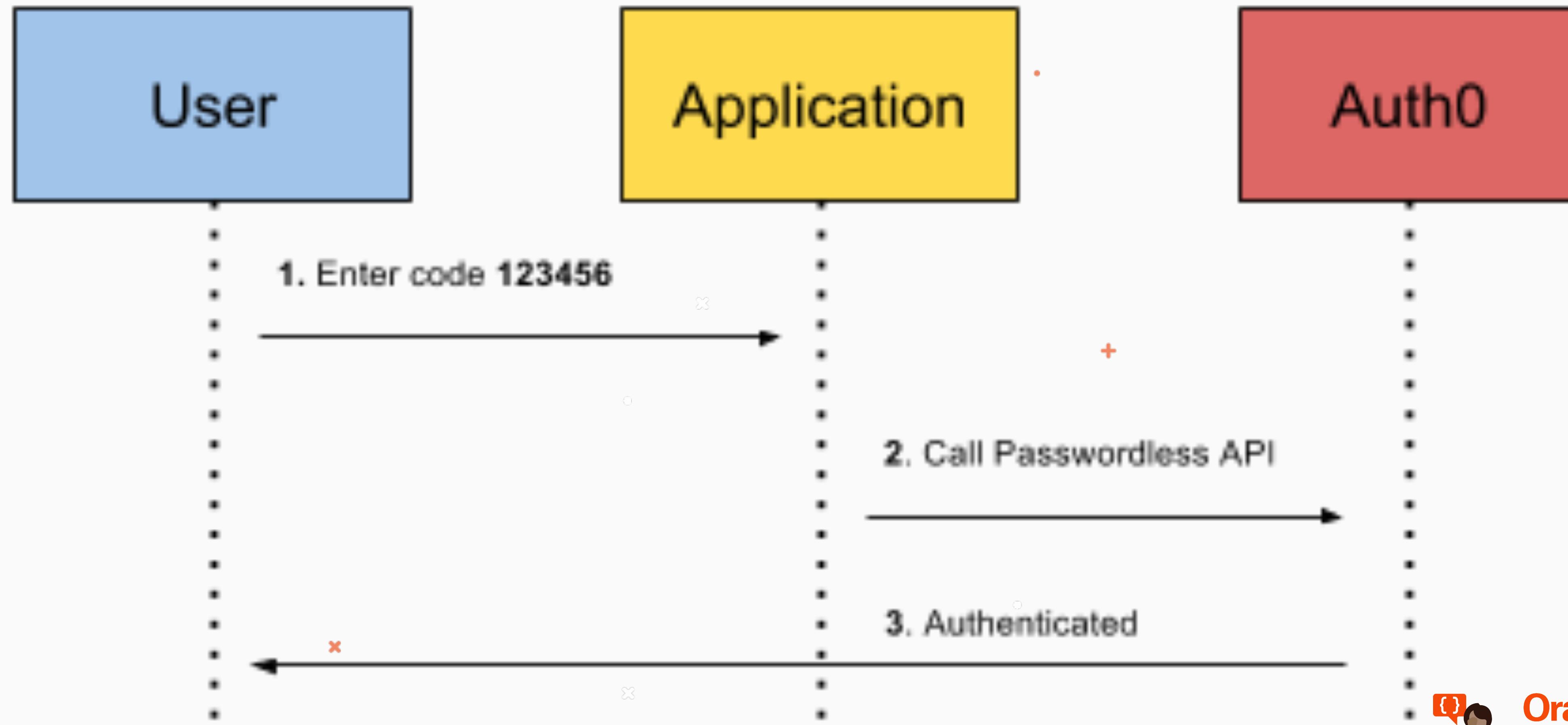
Touch ID



@itrjwyss



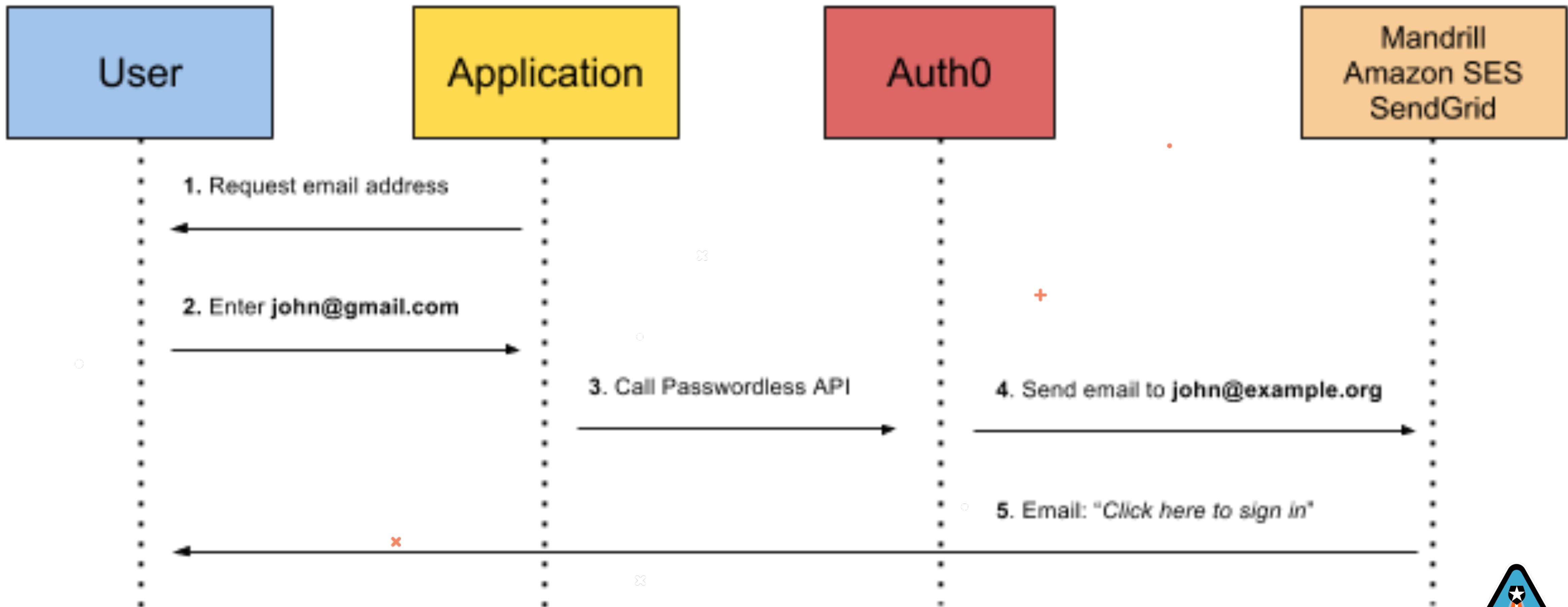
SMS Code



@itrjwyss



Magic Link



@itrjwyss





slack

@itrjwyss

 Oracle
Groundbreaker
Ambassador



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](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



Social Federated Identity

@itrjwyss





Basecamp



Amazon Web
Services



AOL Reader



Auth0
OpenIDConnect



Baidu



Bitbucket



Box



docomo
Docomo

@itrjwyss





Dropbox



Dwolla



Evernote



Exact



Facebook



Fitbit



Github



Goodreads

@itrjwyss



Oracle
Groundbreaker
Ambassador



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





Active
Directory



ADFS



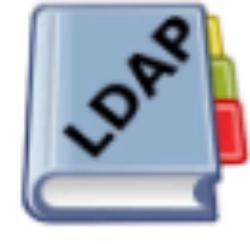
Azure Active
Directory
Native



Google Apps



IP Address
Authentication



LDAP



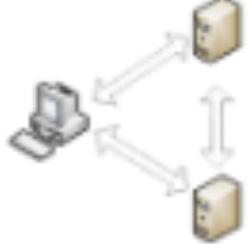
Office 365
(Deprecated)



PingFederate



SharePoint
Apps



WS-Federation



Azure Active
Directory

Legal Federated Identity

@itrjwyss



 bankID

Norwegian
BankID



Swedish
BankID

NEM ID

Danish NemID

@itrjwyss



How to have a successful Identity Management Project

@itrjwyss



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

@itrjwyss



1. How will user accounts be created?

@itrjwyss

Oracle
Groundbreaker
Ambassador.

A photograph of three dolphins leaping out of the ocean. They are dark grey/black on top and white on the bottom. They are positioned diagonally from bottom-left to top-right. The background is a bright blue ocean.

2. Will user profiles need to be synchronized?

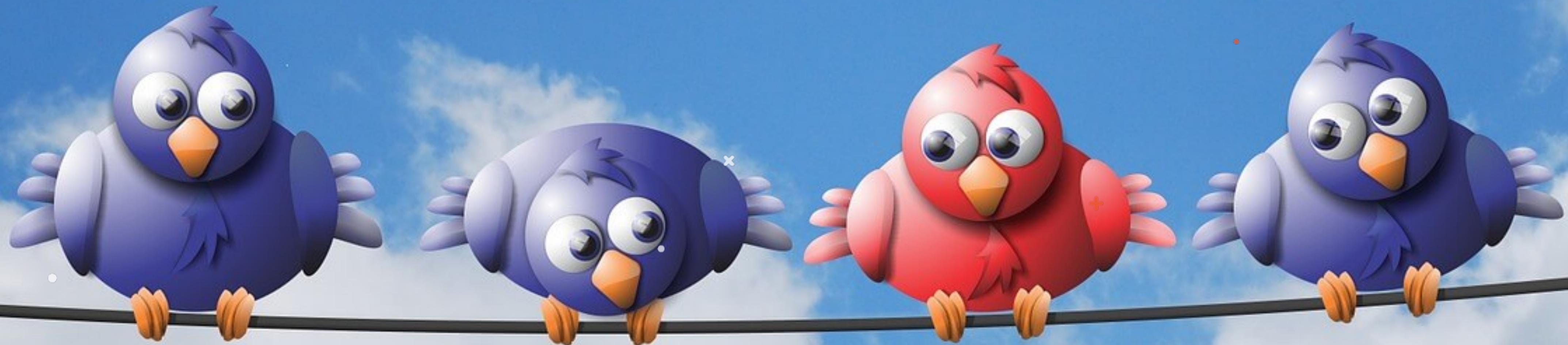
@itrjwyss



@itrjwyss



Oracle
Groundbreaker
Ambassador



3. Username uniqueness

4. How will users Log In?

@itrjwyss



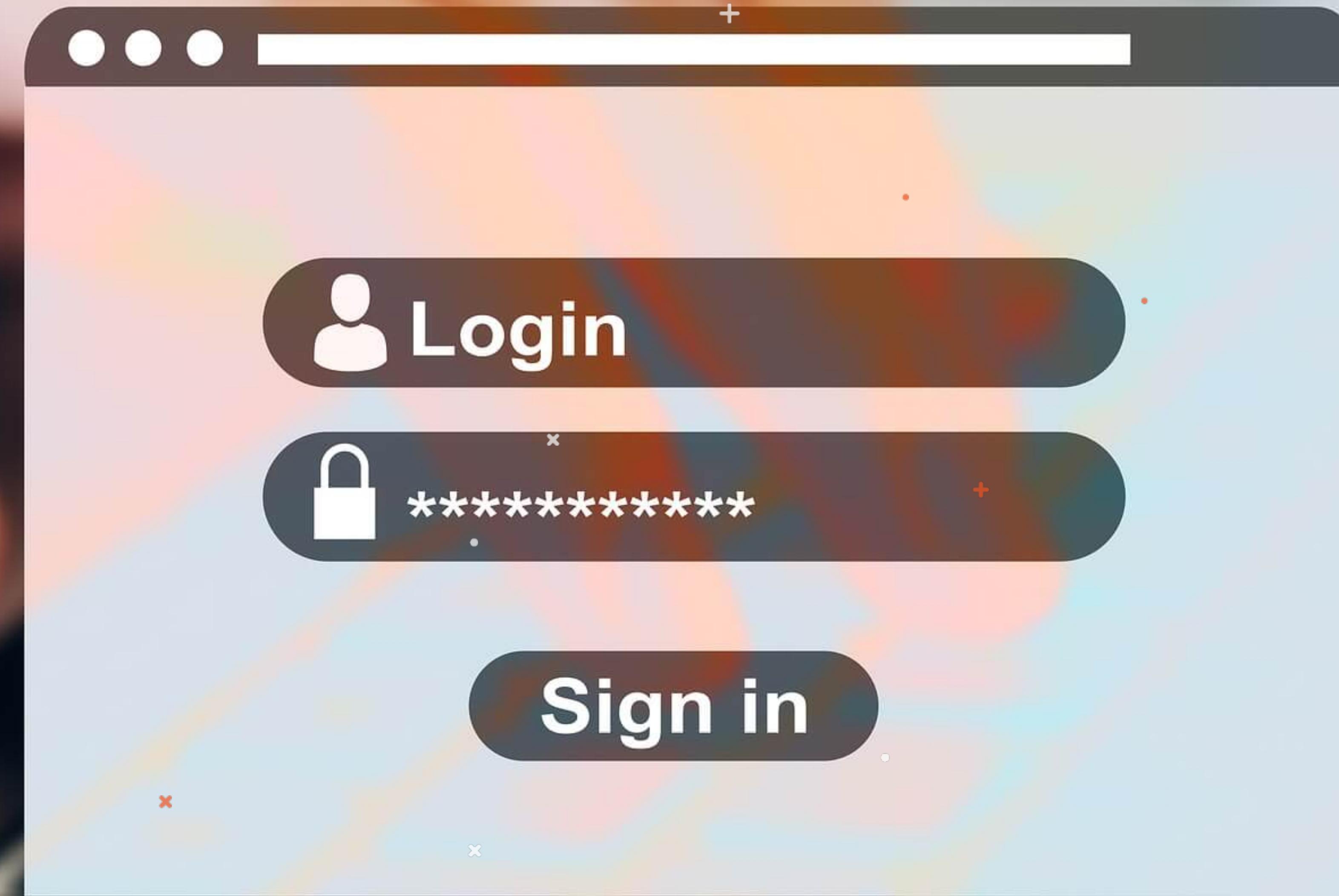
5. Should Multi-Factor Authentication (MFA) be used and if so, When?



@itrjwyss

Oracle
Groundbreaker
Ambassador

6. Is single Sing-On needed?



@itrjwyss



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



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

@itrjwyss

 Oracle
Groundbreaker
Ambassador.

12. Password Reset



@itrjwyss



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



16. Audit Logs

@itrjwyss



Oracle
Groundbreaker
Ambassador



17. Consider how Identity Information might change over time

@itrjwyss



Identity as a Service

.IDaaS

@itrjwyss



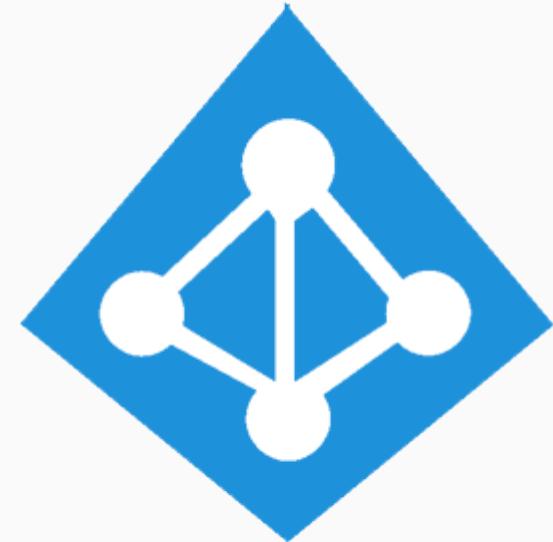
IDaaS

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

@itrjwyss



Popular Clouds



Azure Active Directory

ORACLE
IDENTITY MANAGEMENT



Firebase
Authentication

 **amazon**
web services



Auth0

@itrjwyss

 Oracle
Groundbreaker
Ambassador

Other Popular IDaaS

okta

WSO₂

@itrjwyss



Other IDaaS



onelogin



@itrjwyss

Oracle
Groundbreaker
Ambassador

Other Providers



@itrjwyss



Architecture Level

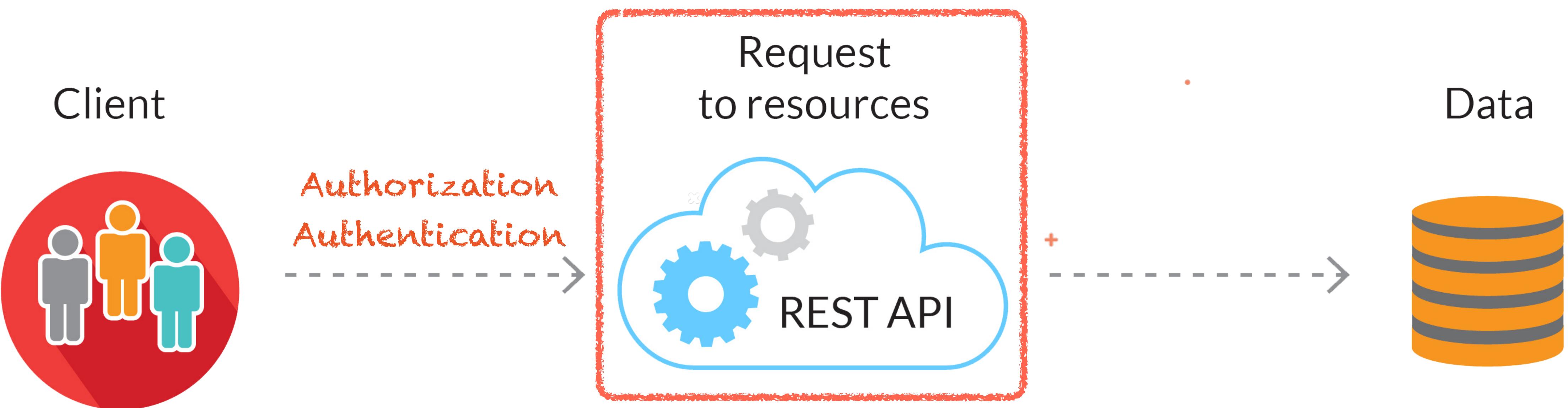
@itrjwyss

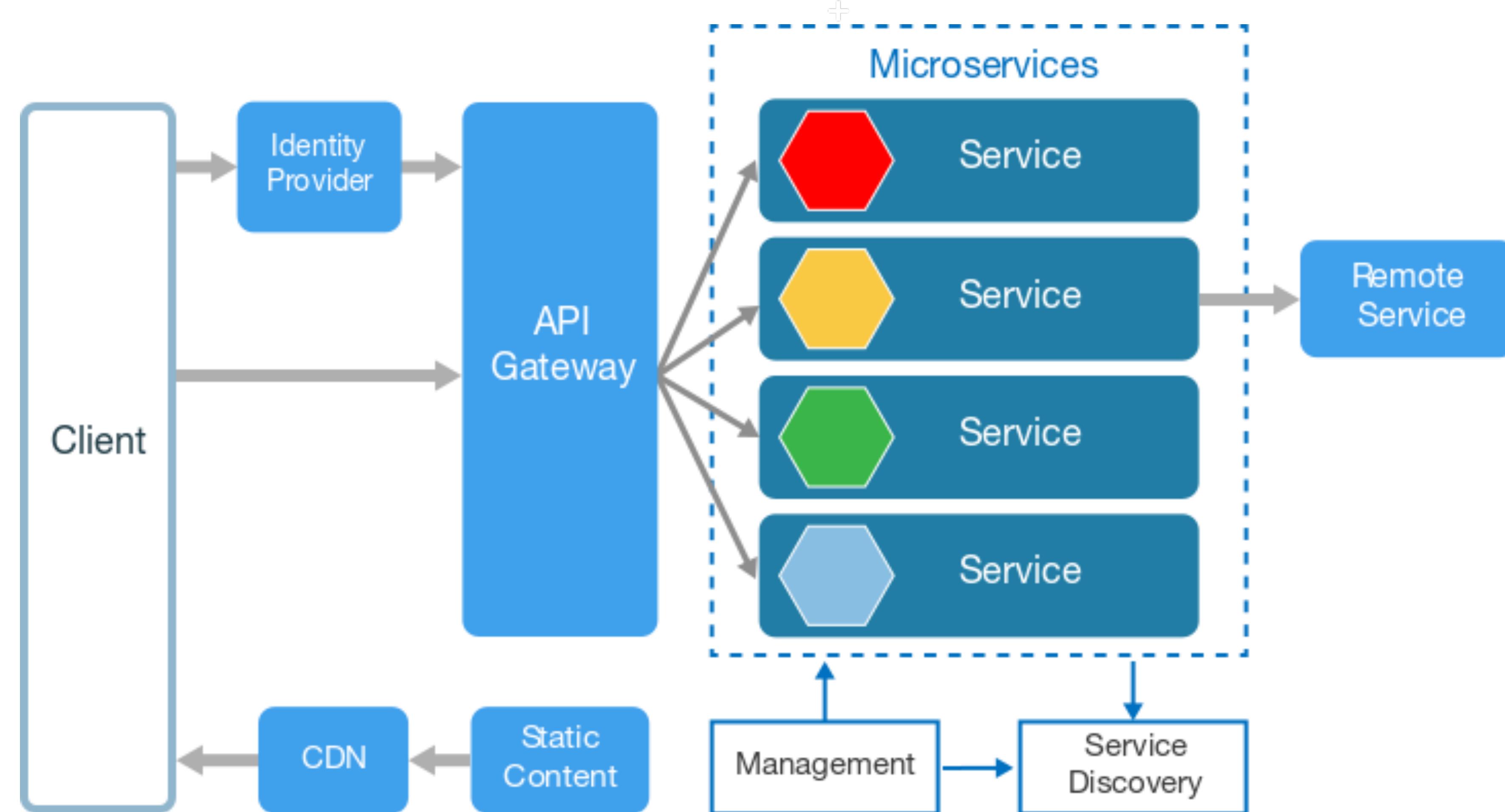


Developing REST APIs

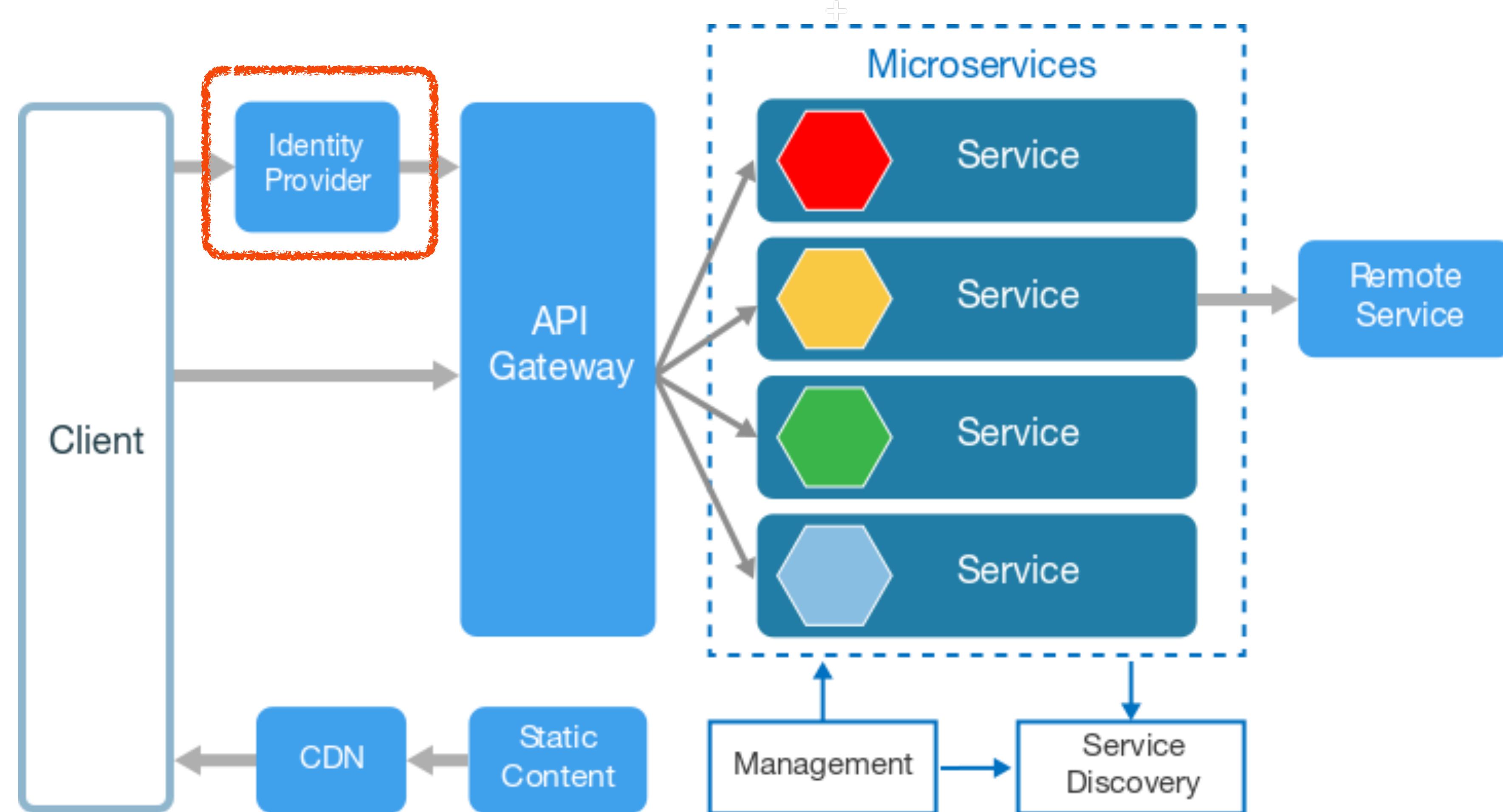


Developing REST APIs

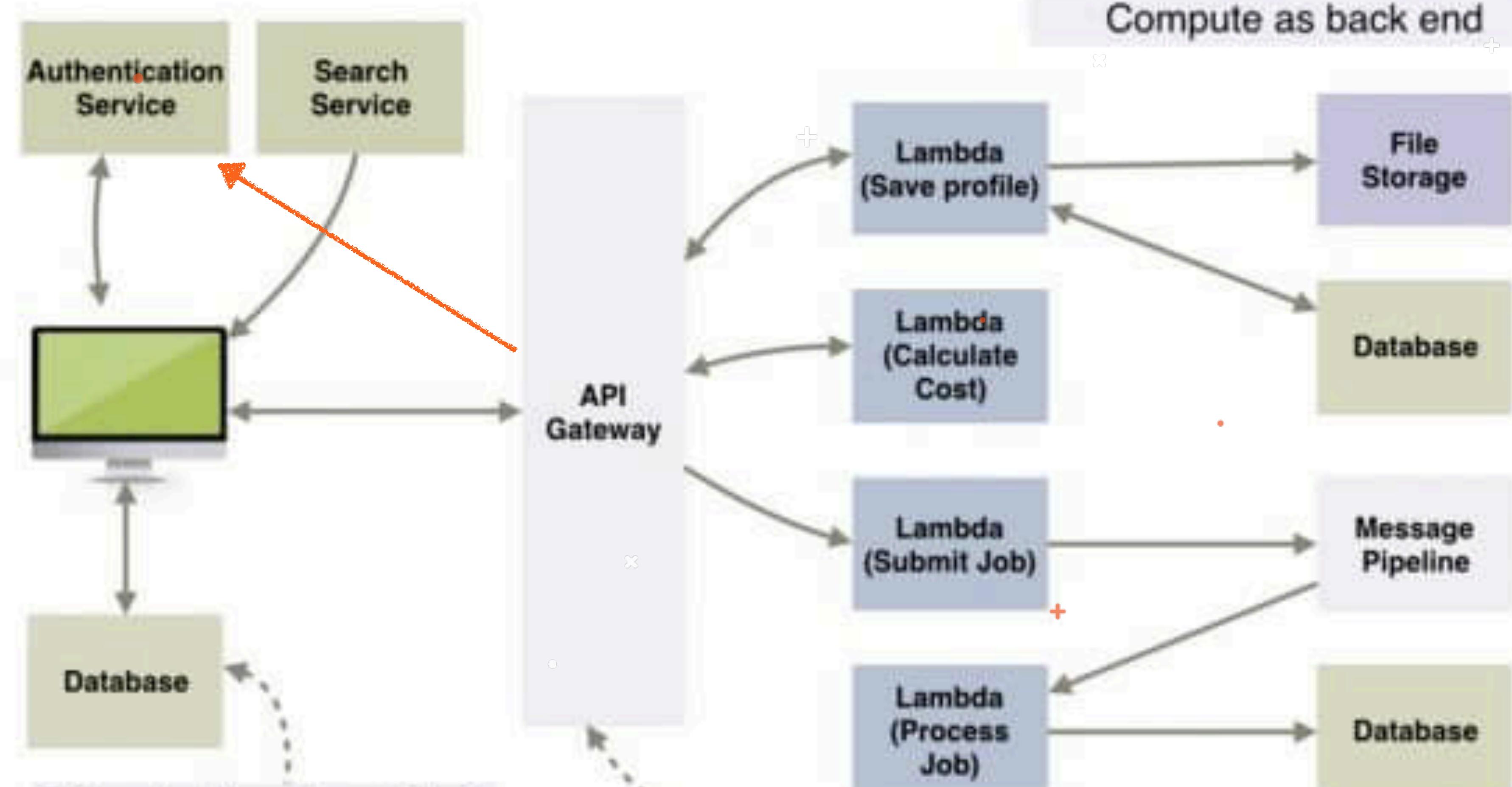




@itrjwyss

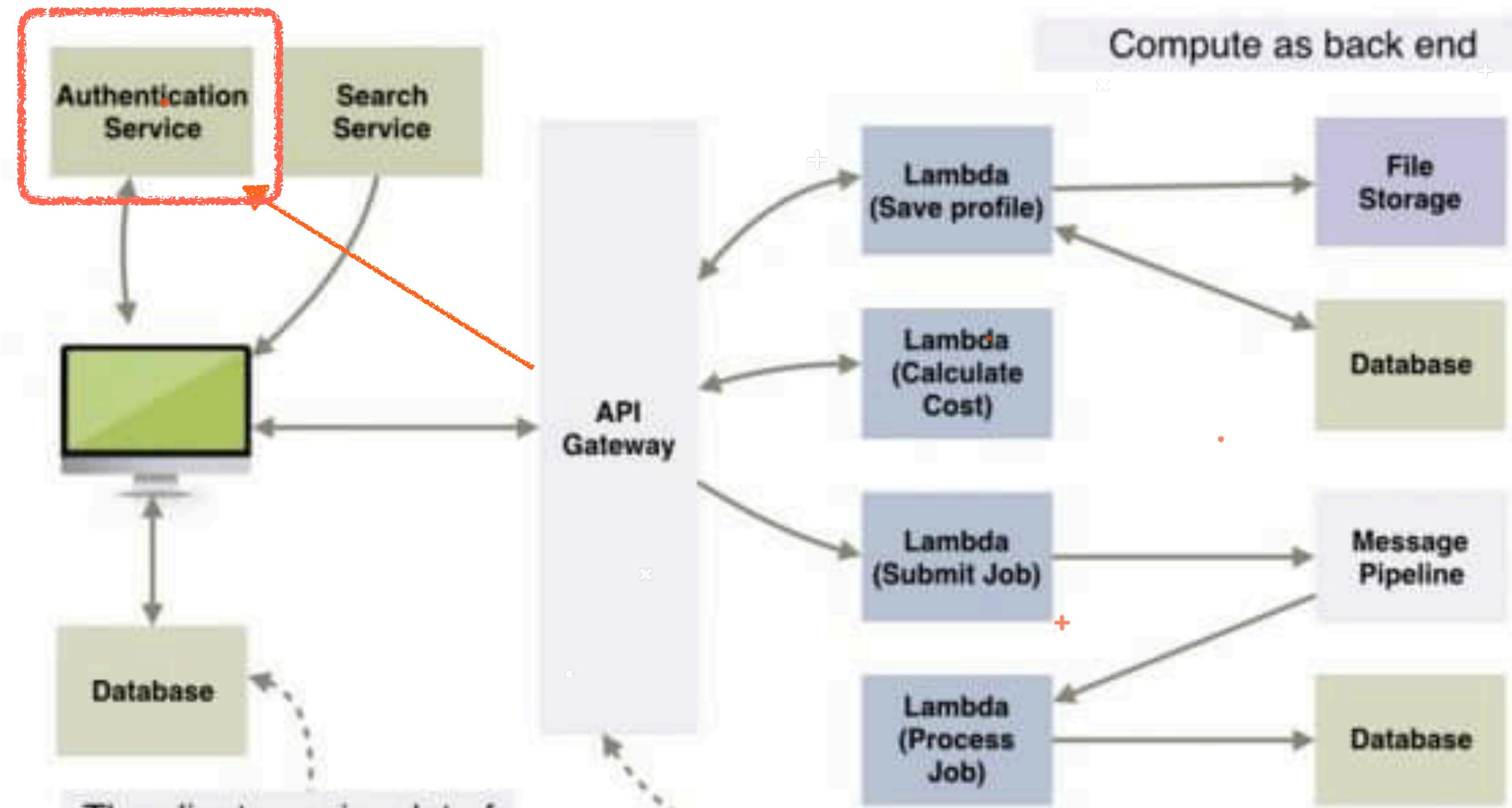


@itrjwyss



The client can, in a lot of cases, communicate with services **directly** rather than relaying through the API Gateway.

The API Gateway creates a RESTful interface and hides Lambda functions and other services behind it. Lambda functions can carry out custom tasks and communicate with other services.



The client can, in a lot of cases, communicate with services **directly** rather than relaying through the API Gateway.

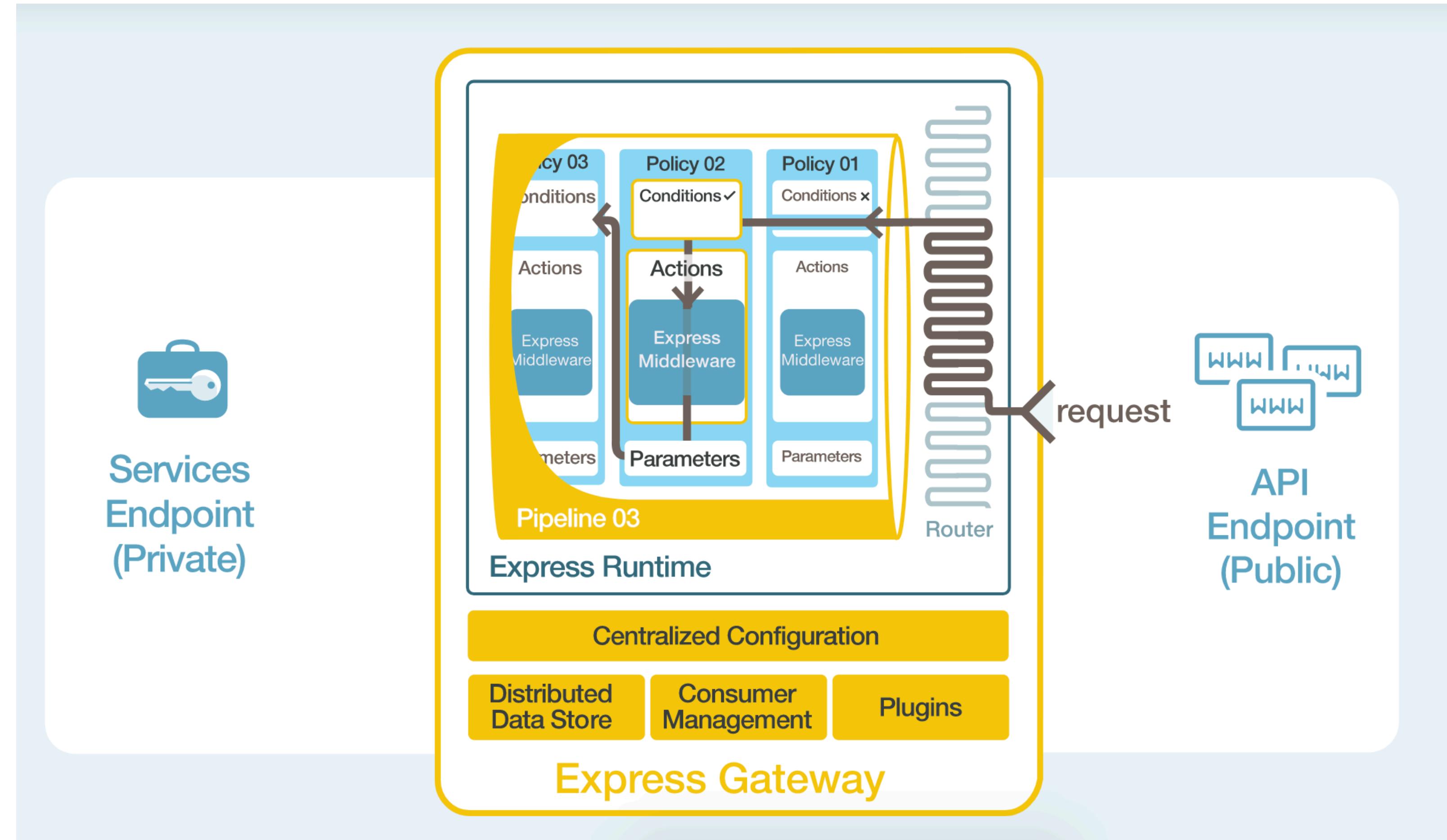
The API Gateway creates a RESTful interface and hides Lambda functions and other services behind it. Lambda functions can carry out custom tasks and communicate with other services.

Practical Case

@itrjwyss



Express Gateway



@itrjwyss



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

<https://www.facebook.com/itrjwyss>

@itrjwyss

@itrjwyss

