Modern Identity Management

In the era of Serverless and Microservices

Security Matters

@itrwyss

US Data Breaches Statistics

First half of 2019

54%
Increase

3,800+
were reported

3.2 billion
Just 8 of those

@itrwyss

@itrwyss

Had Been Uploaded

38,000
Driver’s Licenses

3,200
Passport Details

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

@itrwyss

GDPR

Data Protection Officer (DPO)

Compliance

25. maj 2018

Databrud

Persondata

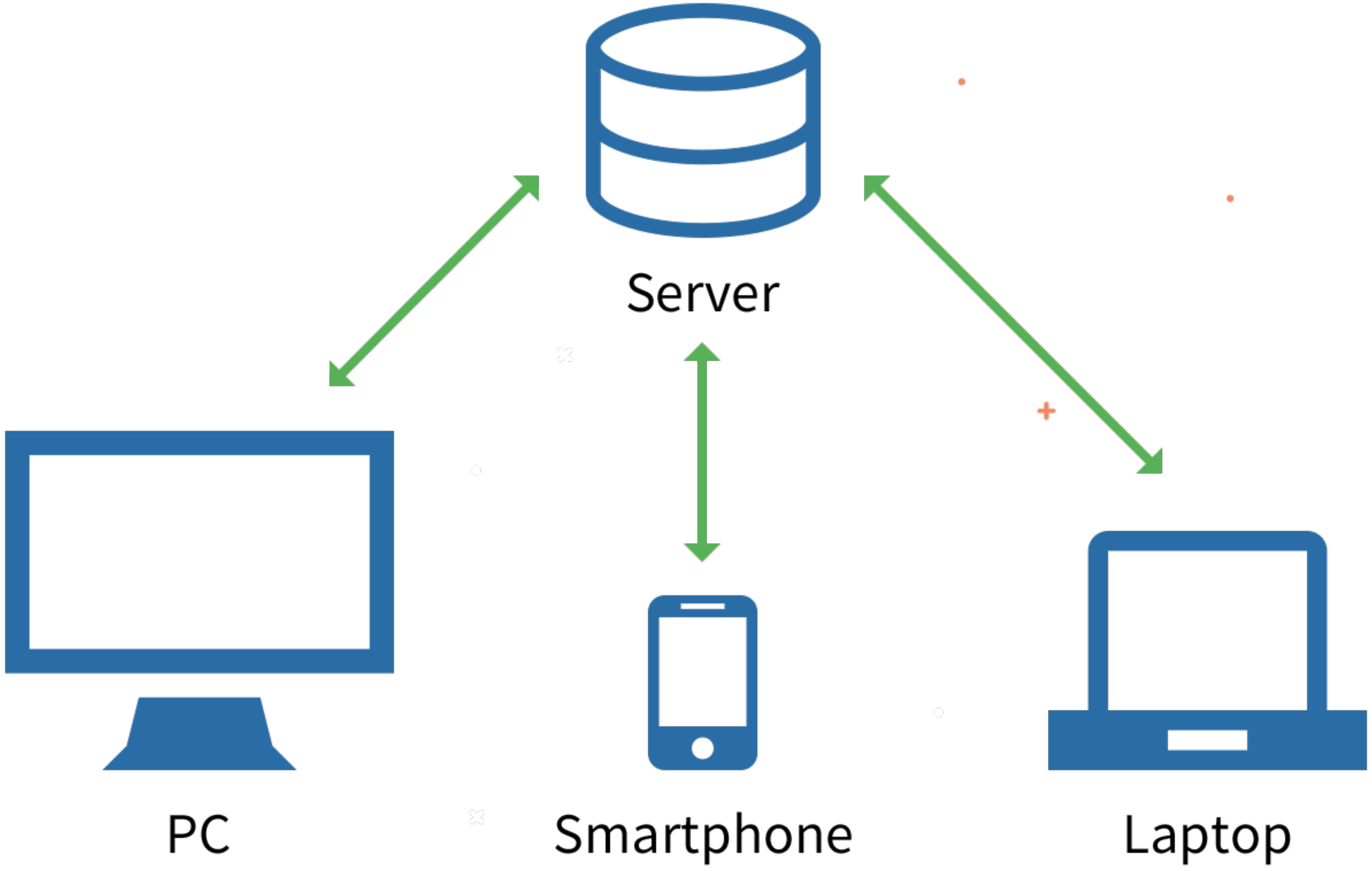
The EU - U.S. Privacy Shield

TrustArc

Security **must** be a goal.

@itrwyss

Security is a **Team Effort**



@itrwyss

Best Practices

Identity ~~Security~~

@itrwyss

Talk Roadmap

- Rest API Design / OAuth
- JWT (JSON Web Tokens)
- 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
- Demo

Mercedes Wyss
@itrjwyss

Community Leader
Devs+502 & JDuchess Guatemala

Mozilla Hispano & Guatemala

Chief Technology Officer (CTO) at Produactivity
Full Stack Developer
(Backend, Android, Frontend)

Auth0 Ambassador &
Oracle Groundbreaker Ambassador

Duke's Choice Award
2016 Winner
Java

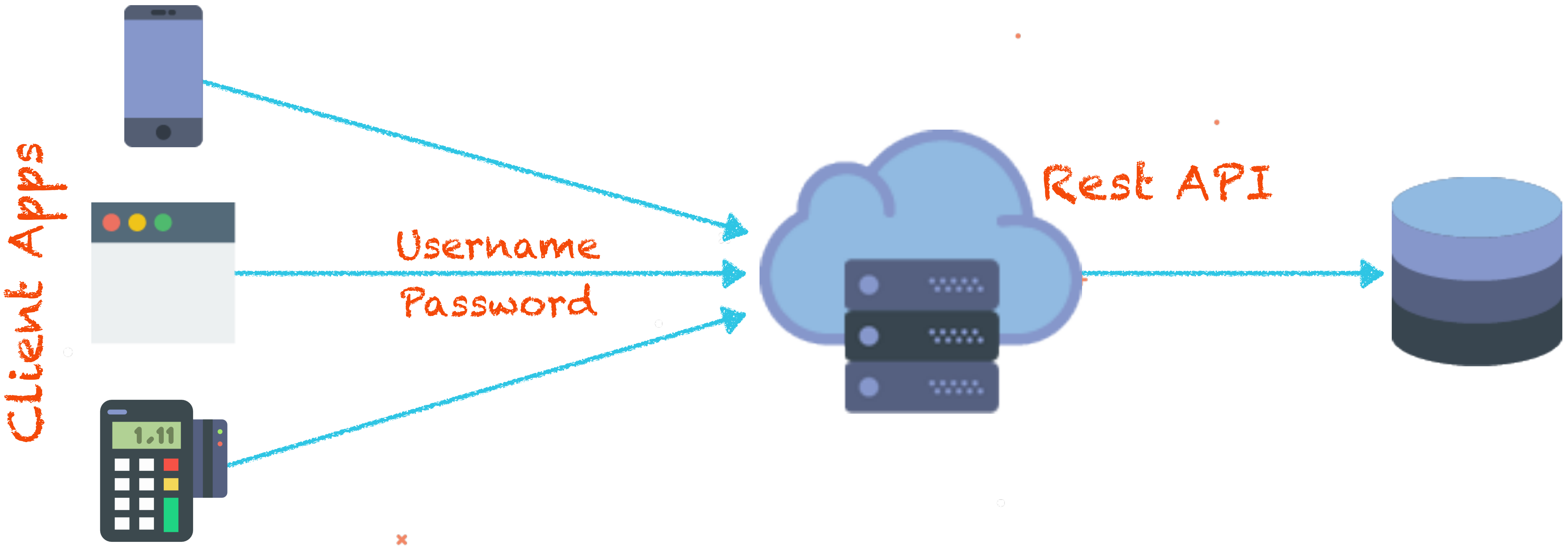
AMBASSADOR

Oracle Groundbreaker Ambassador

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

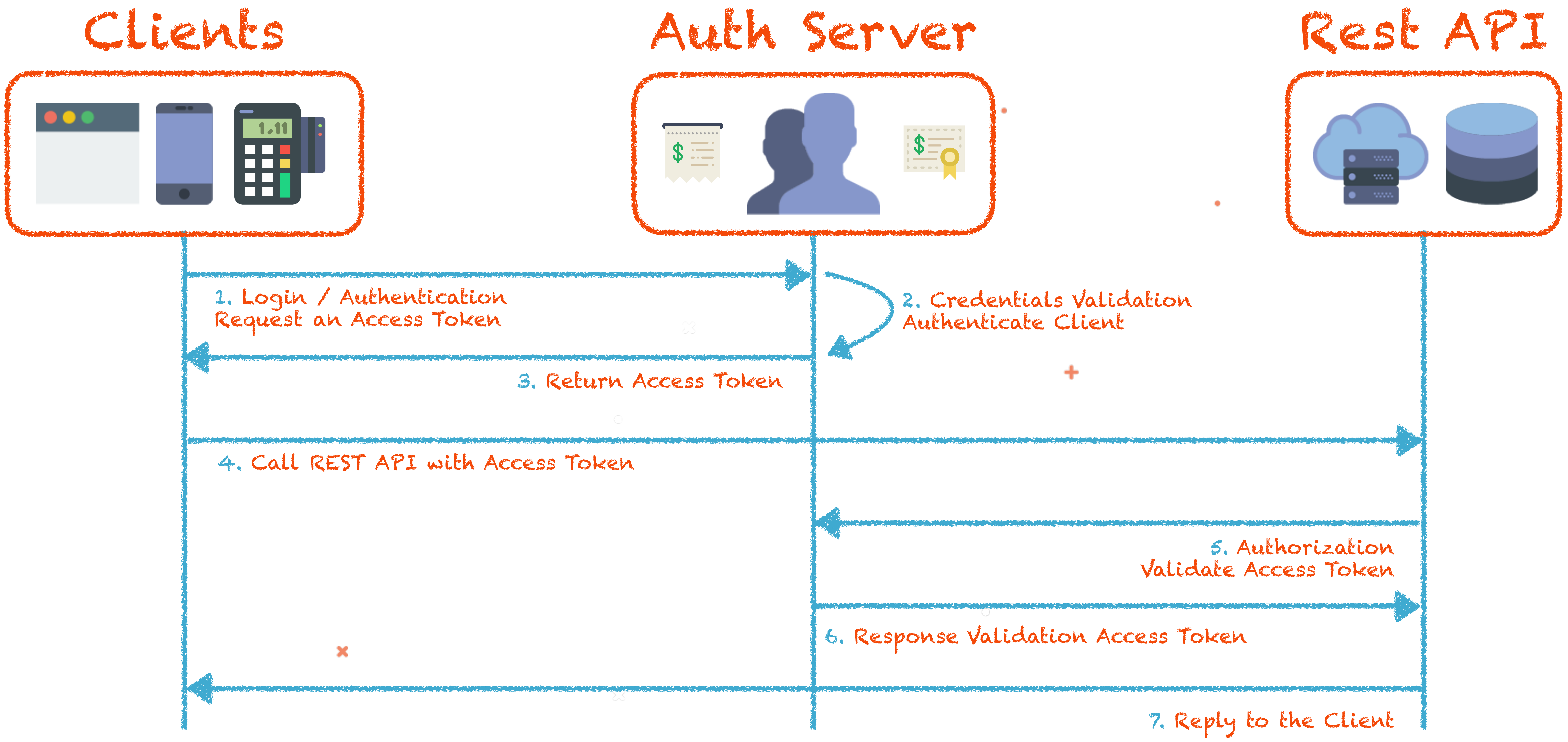
JDuchess Guatemala

Bad API Design



@itrwyss

OAuth



Clients

Auth Server

Rest API

1. Login / Authentication
Request an Access Token

2. Credentials Validation
Authenticate Client

3. Return Access Token

4. Call REST API with Access Token

5. Authorization
Validate Access Token

6. Response Validation Access Token

7. Reply to the Client

@itrwyss

J W T

@itrwyss

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

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ
9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZ
SI6IkpvaG4gRG9lIiwiYWRtaW4iOnRy
dWV9 TJVA95OrM7E2cBab30RMHrHDc
EfxjoYZgeFONFh7HgQ

Claims

@itrwyss

JSON Web Signature

JWT + JWS

@itrwyss

Signature Algorithms

JWS

JWS	Algorithm	Description
HS256	HMAC256	HMAC with SHA-256
HS384	HMAC384	HMAC with SHA-384
HS512	HMAC512	HMAC with SHA-512
RS256	RSA256	RSASAA-PKCS1-v1_5 with SHA-256
RS384	RSA394	RSASAA-PKCS1-v1_5 with SHA-384
RS512	RSA512	RSASAA-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-512 and SHA-512

Exploring JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9 Header
.
eyJqdGkiOiI1MWQ4NGFjMS1kYjMxLTRjM2ItOTQwOS1lNjMwZWJiYj
gzZGYiLCJ1c2VybmFtZSI6Imh1bnRlcjIiLCJzY29wZXMiOlsicmVw
bzpyZWFkIiwiZ2lzdDp3cml0ZSJdLCJpc3MiOiIxNDUyMzQzMzcyIi
wiZXhwIjoiMTQ1MjM0OTM3MiJ9 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
)
```

Registered Claims

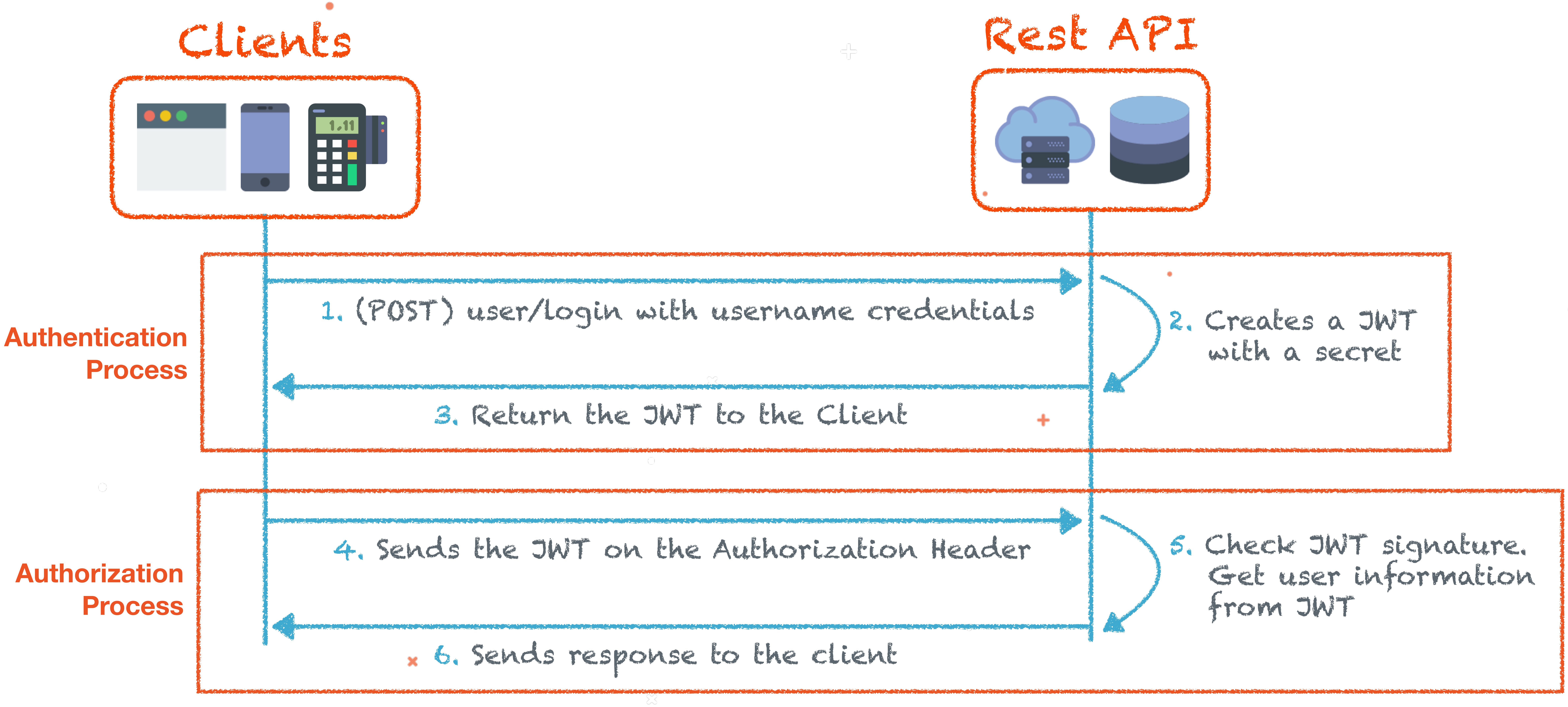
JWT

Claim	Description
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

@itrwyss



Clients
Rest API
Authentication Process
1. (POST) user/login with username credentials
2. Creates a JWT with a secret
3. Return the JWT to the Client
Authorization Process
4. Sends the JWT on the Authorization Header
5. Check JWT signature. Get user information from JWT
6. Sends response to the client

@itrwyss

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",
```

@itrwyss

JWT HANDBOOK

By Sebastián Peyrott

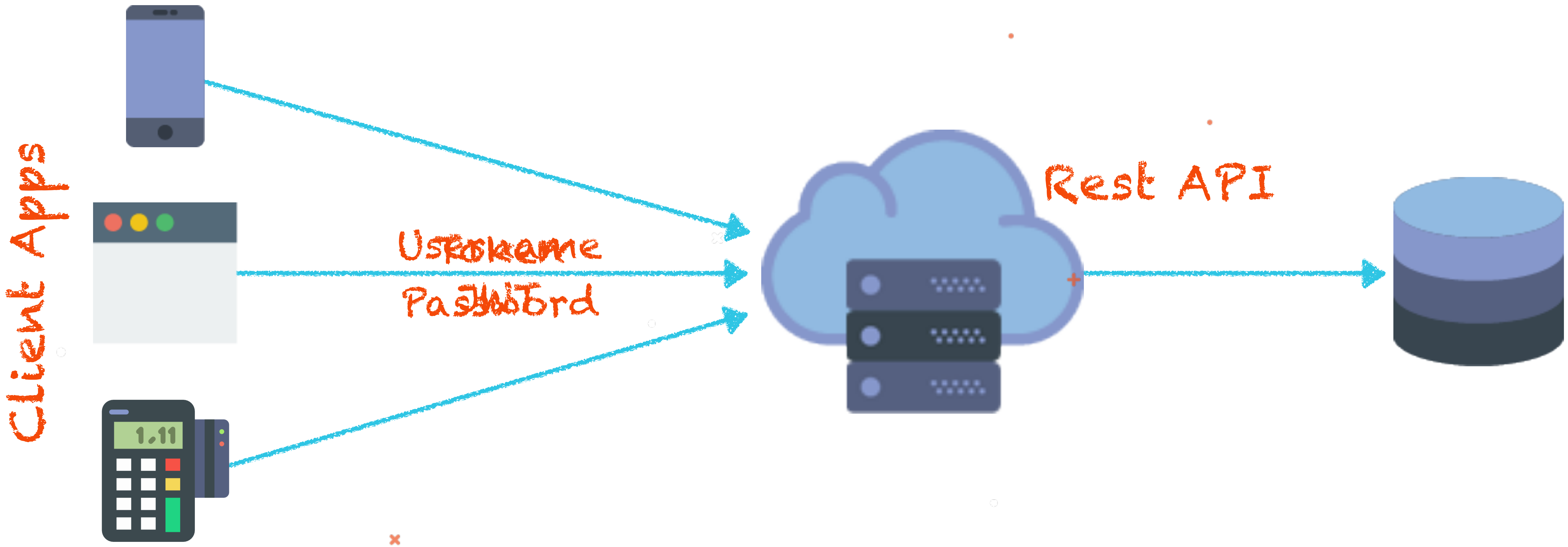
Auth0

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

auth0.com/e-books/jwt-handbook

@itrwyss

Improve API Design



@itrwyss

User Credentials Problem

@itrwyss

SSO

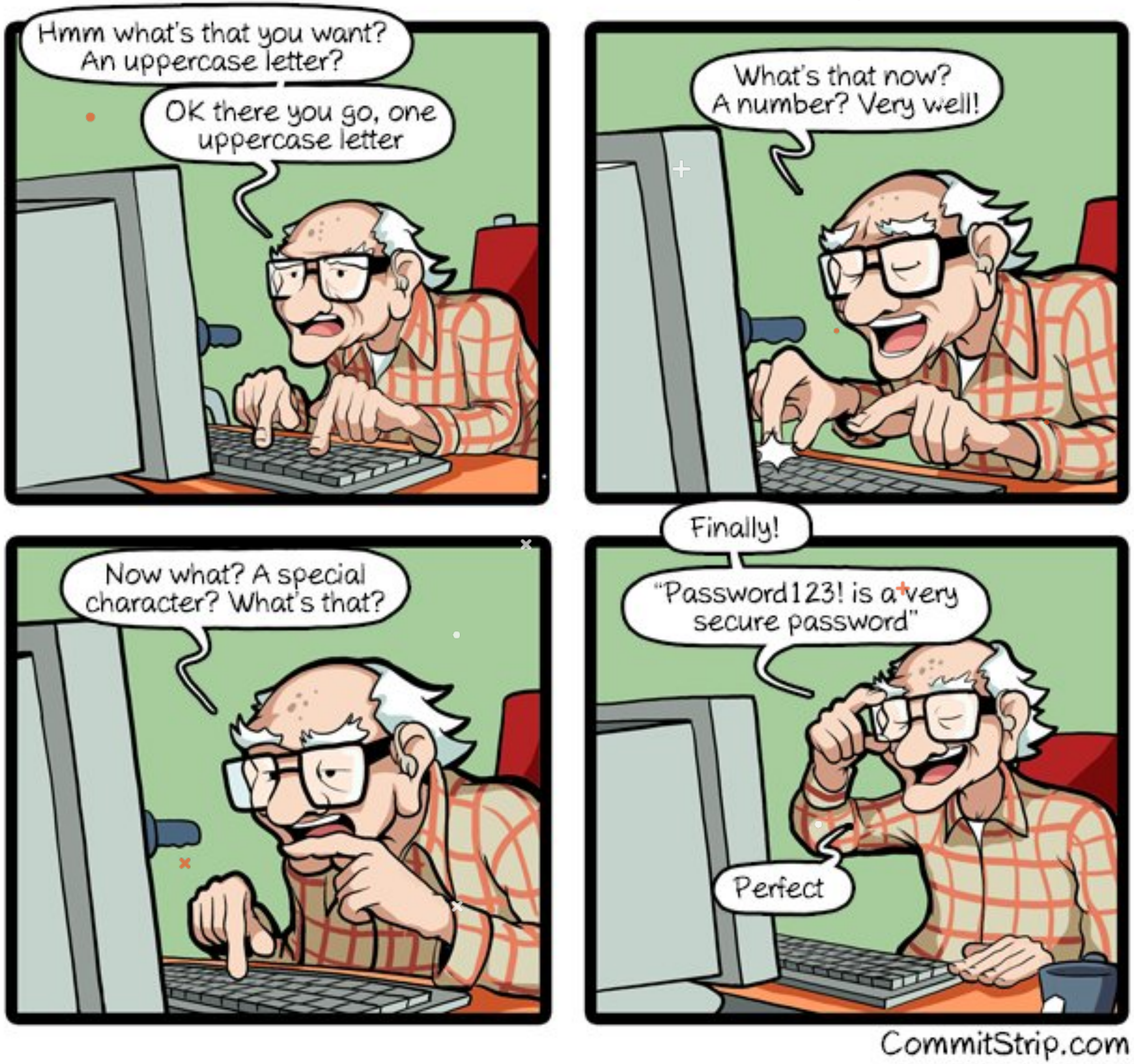
Single Sign On

@itrwyss

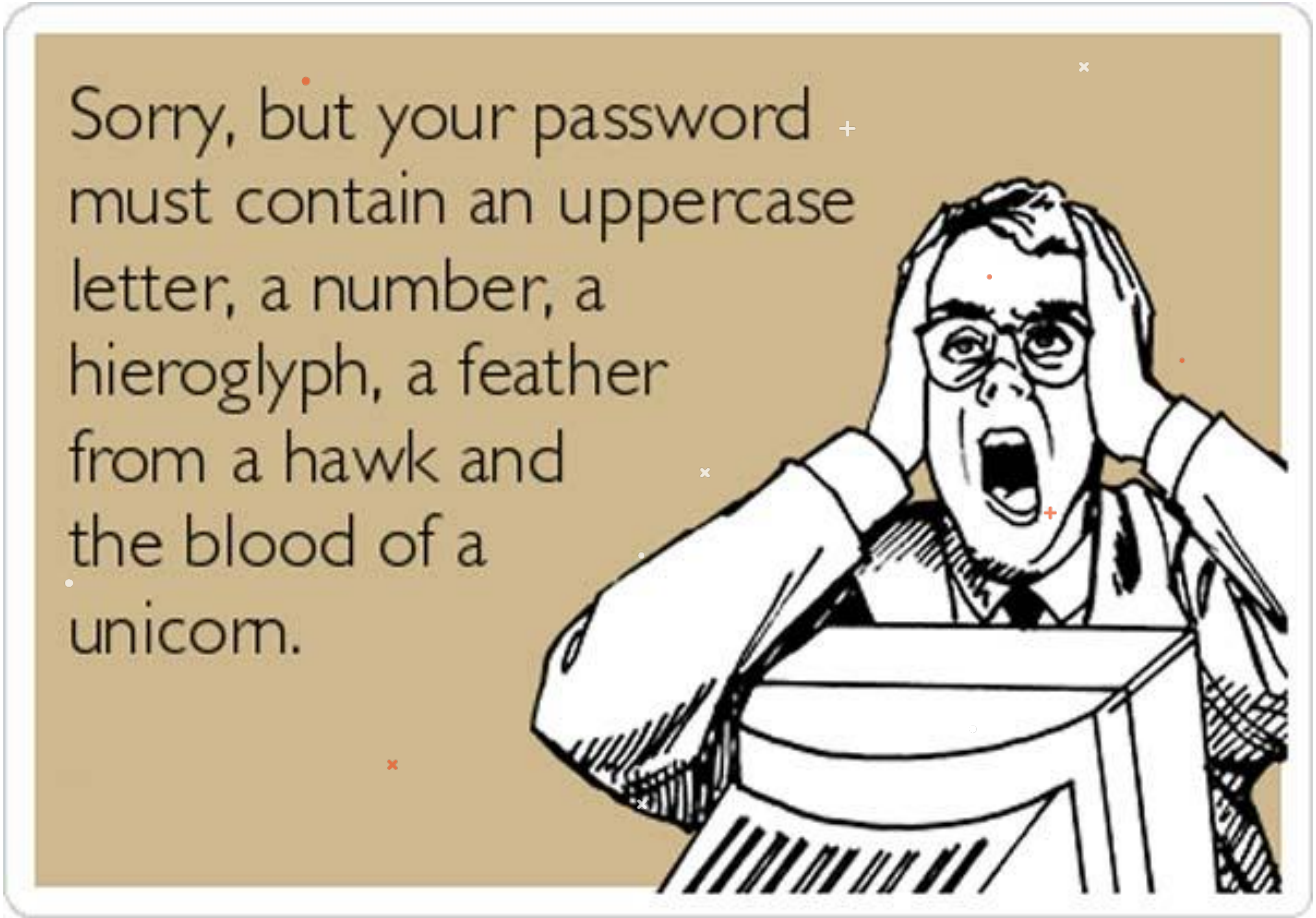
@itrwyss

RULES

@itrwyss

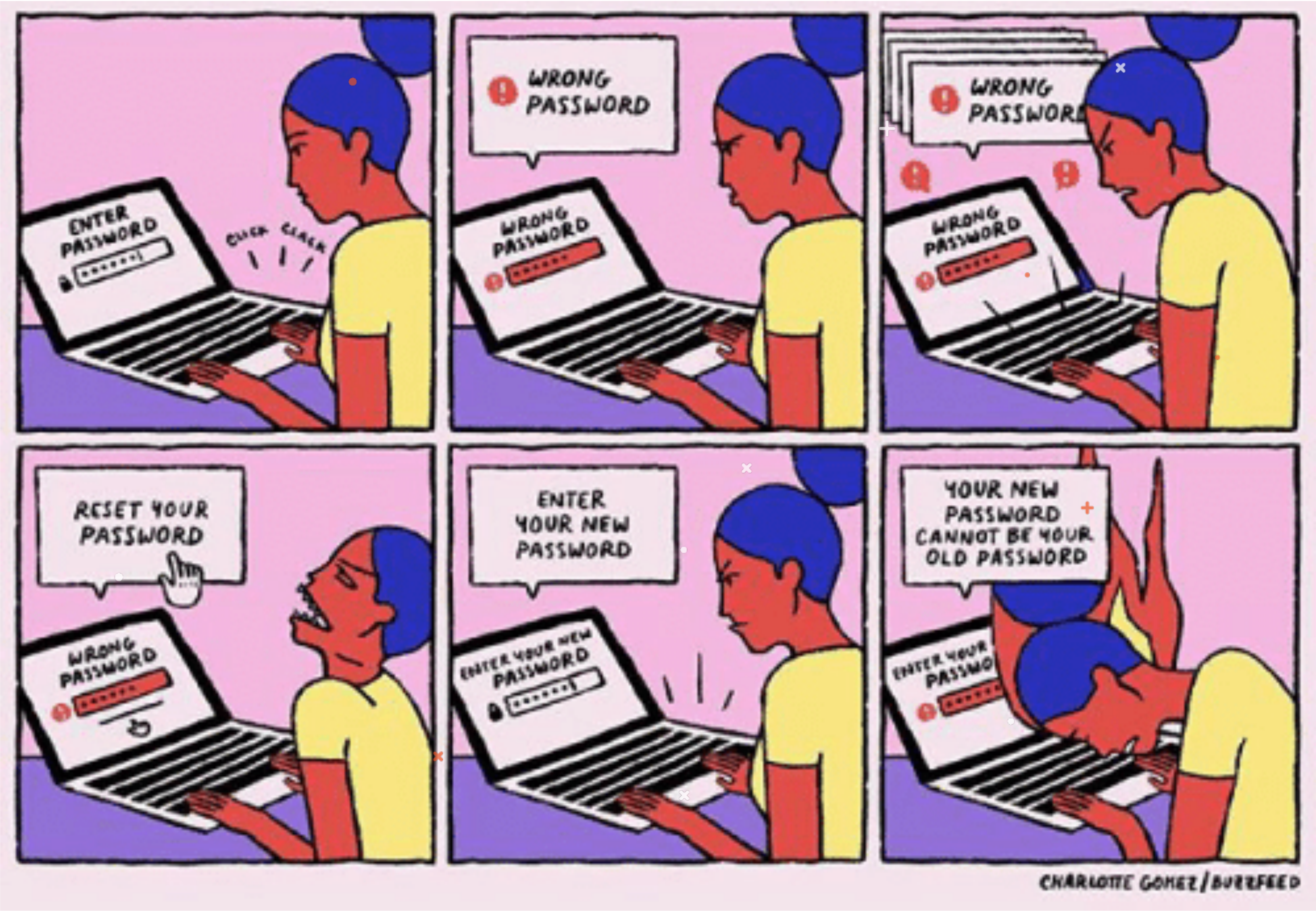

Hmm what's that you want? An uppercase letter?
OK there you go, one uppercase letter
What's that now? A number? Very well!
Now what? A special character? What's that?
Finally!
"Password123! is a very secure password"
Perfect
CommitStrip.com

@itrwyss



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

@itrwyss


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
ENTER YOUR PASSWO
CHARLOTTE GOMEZ / BUZZFEED

@itrwyss

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
ENTER YOUR PASSWO
CHARLOT

@itrwyss

What we can do to improve this process?

Making it **easier** and **safer**.

Identity Management (IdM)

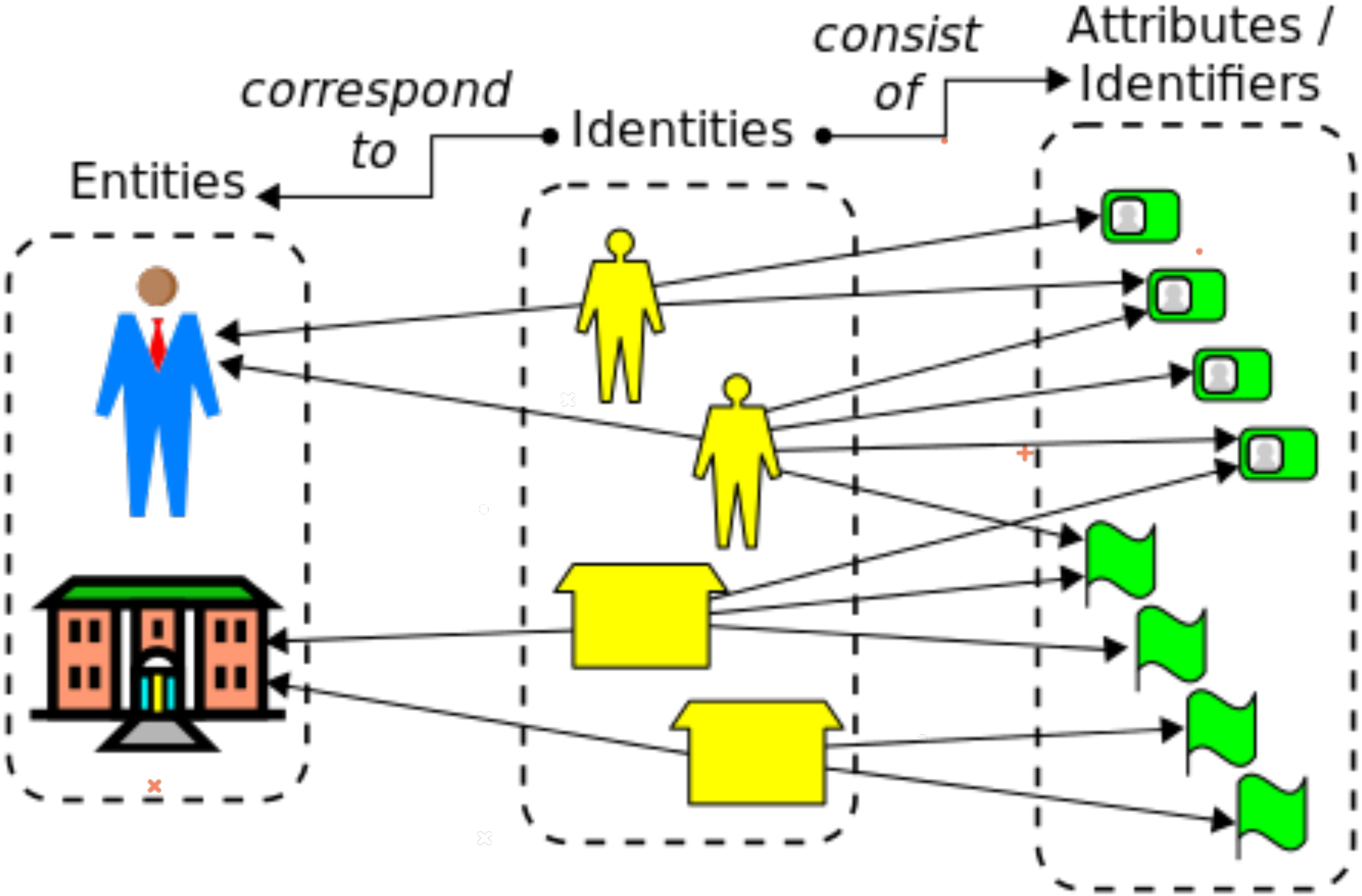
Is an Umbrella term for all of the core logic around identity in a corporate environment.

- Provisioning
- Account management
- Identity governance

@itrwyss

Provisioning

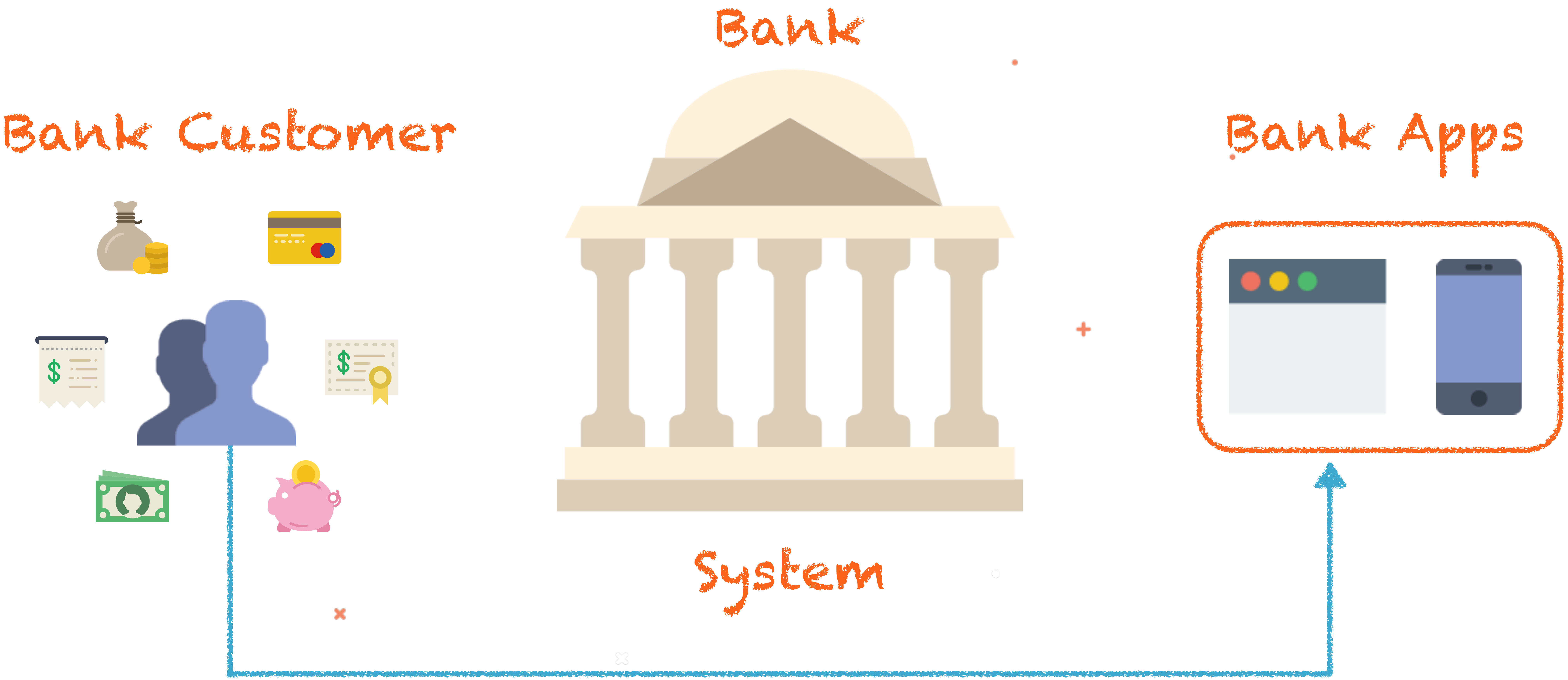
IdM



@itrwyss

Actor = User

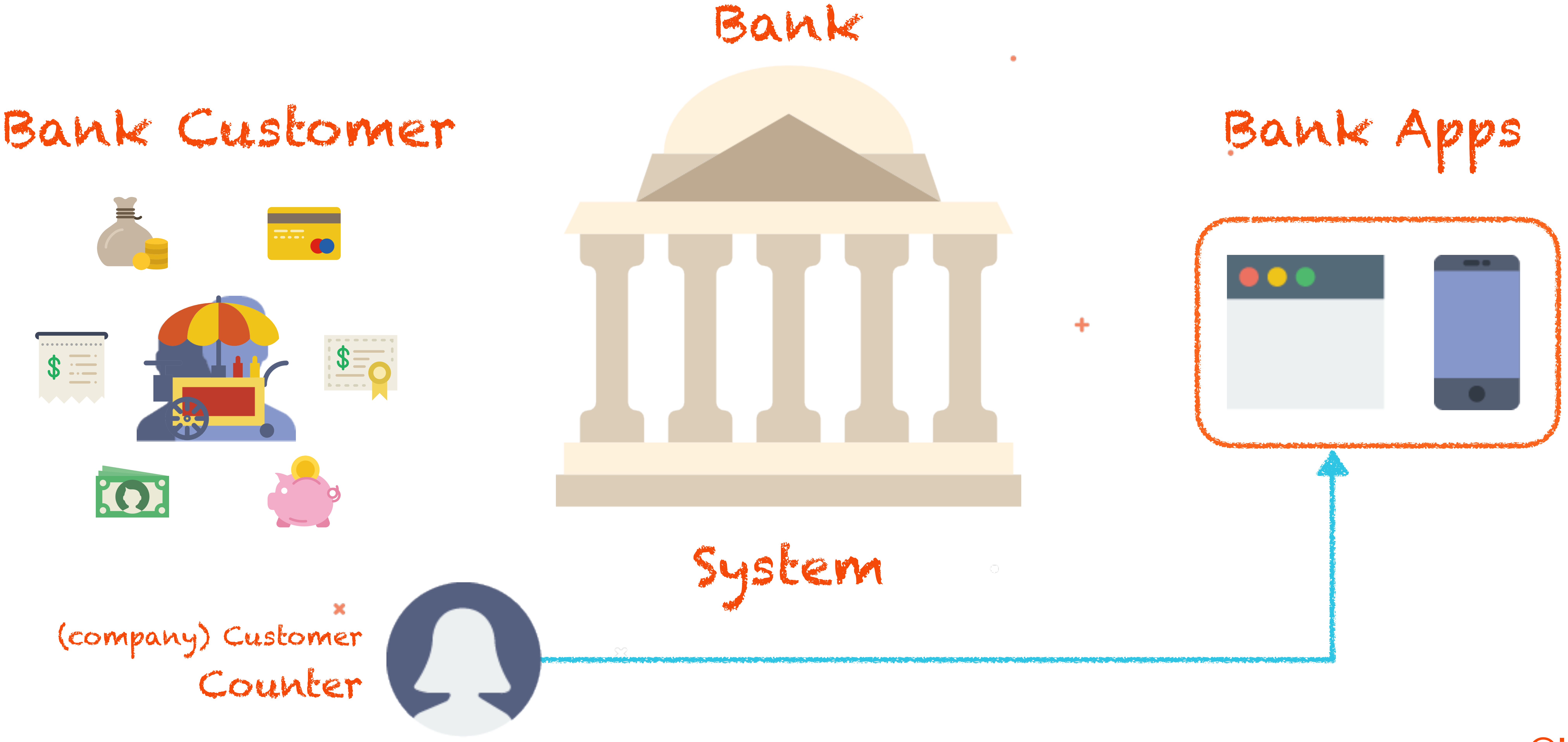
Provisioning



@itrwyss

Actor ≠ User

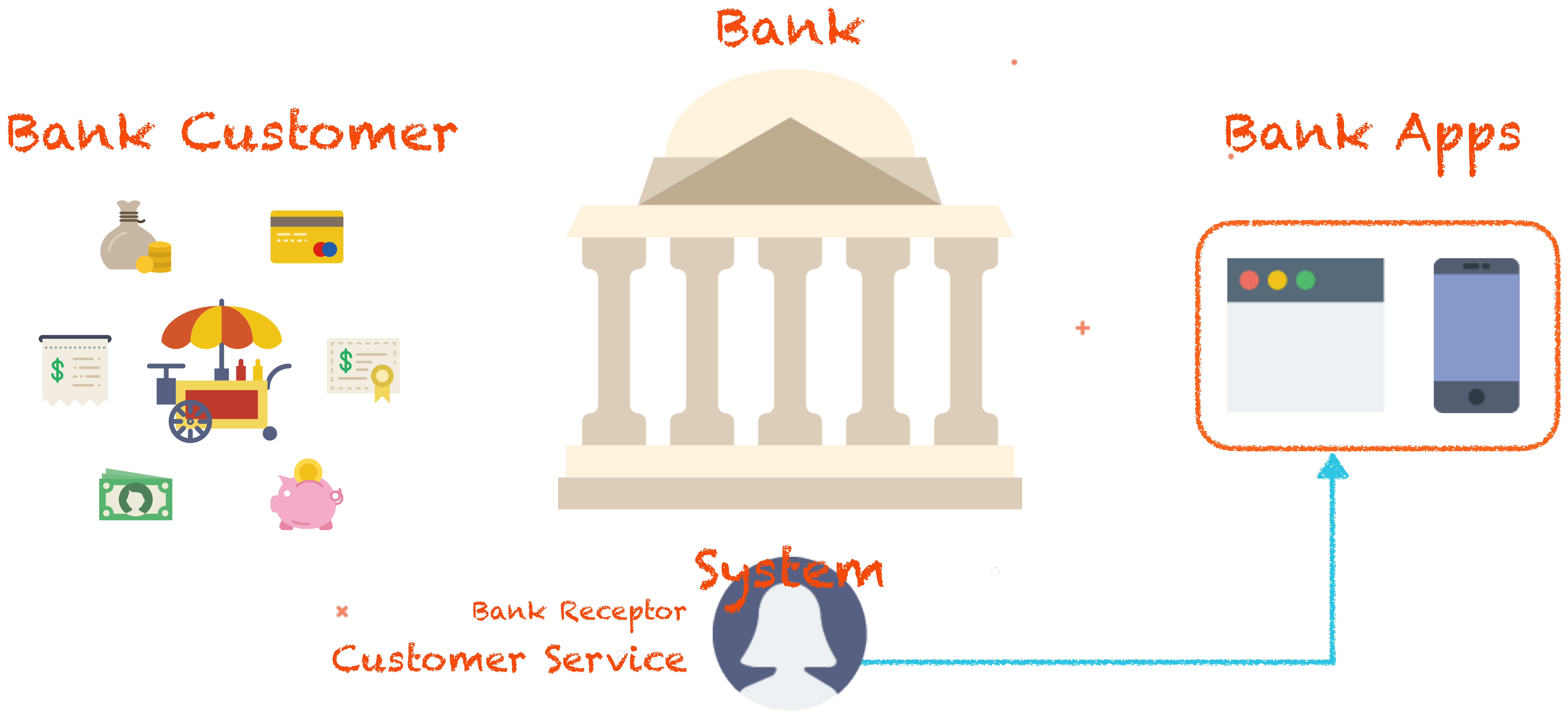
Provisioning



@itrwyss

Actor ≠ User

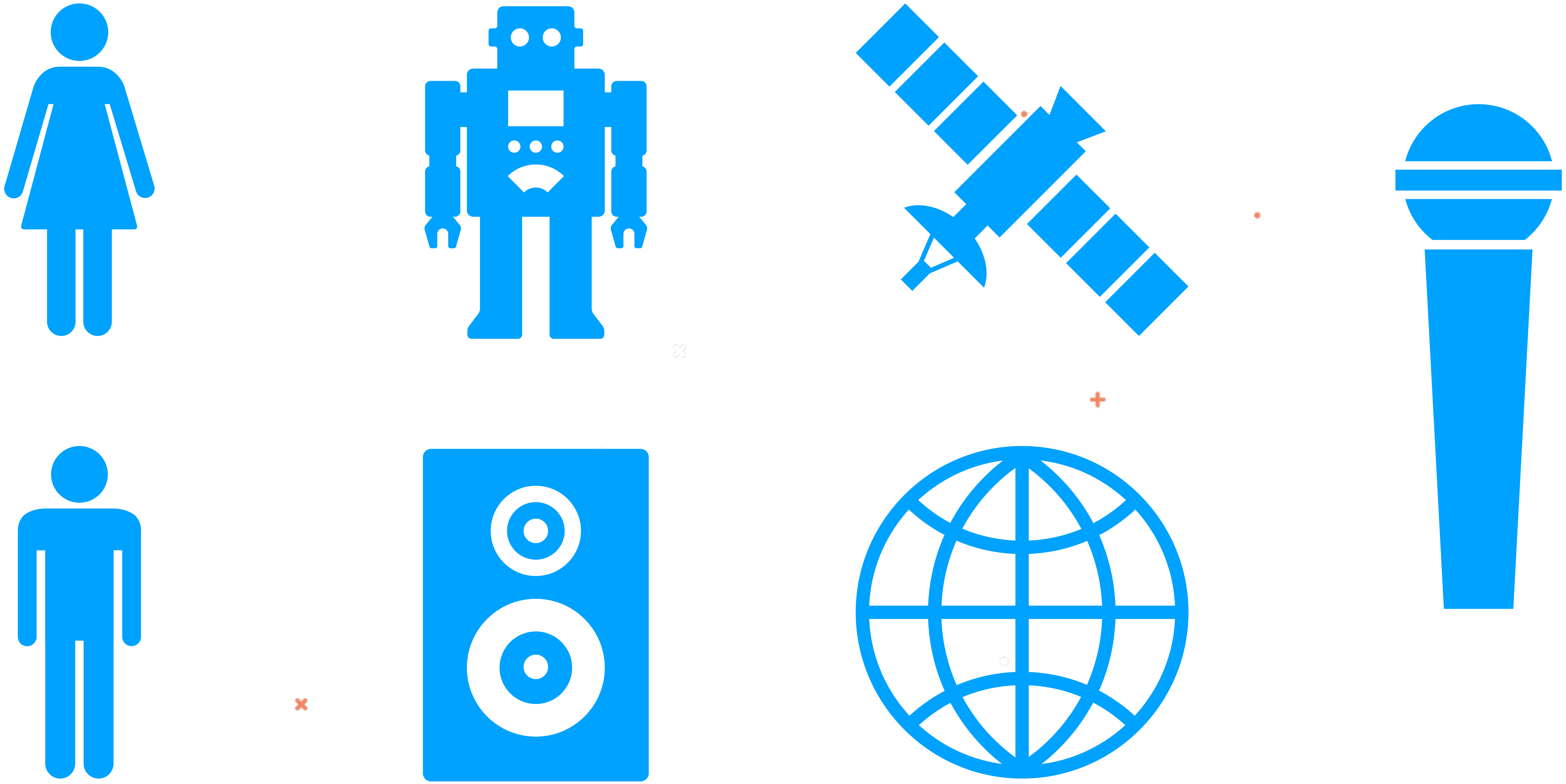
Provisioning



@itrwyss

Provisioning

IdM



@itrwyss

Account Management

IdM

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

Identity Governance

IdM

Assigning them to groups and roles, 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

@itrwyss

Authorization

IAM

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

Identity Federation

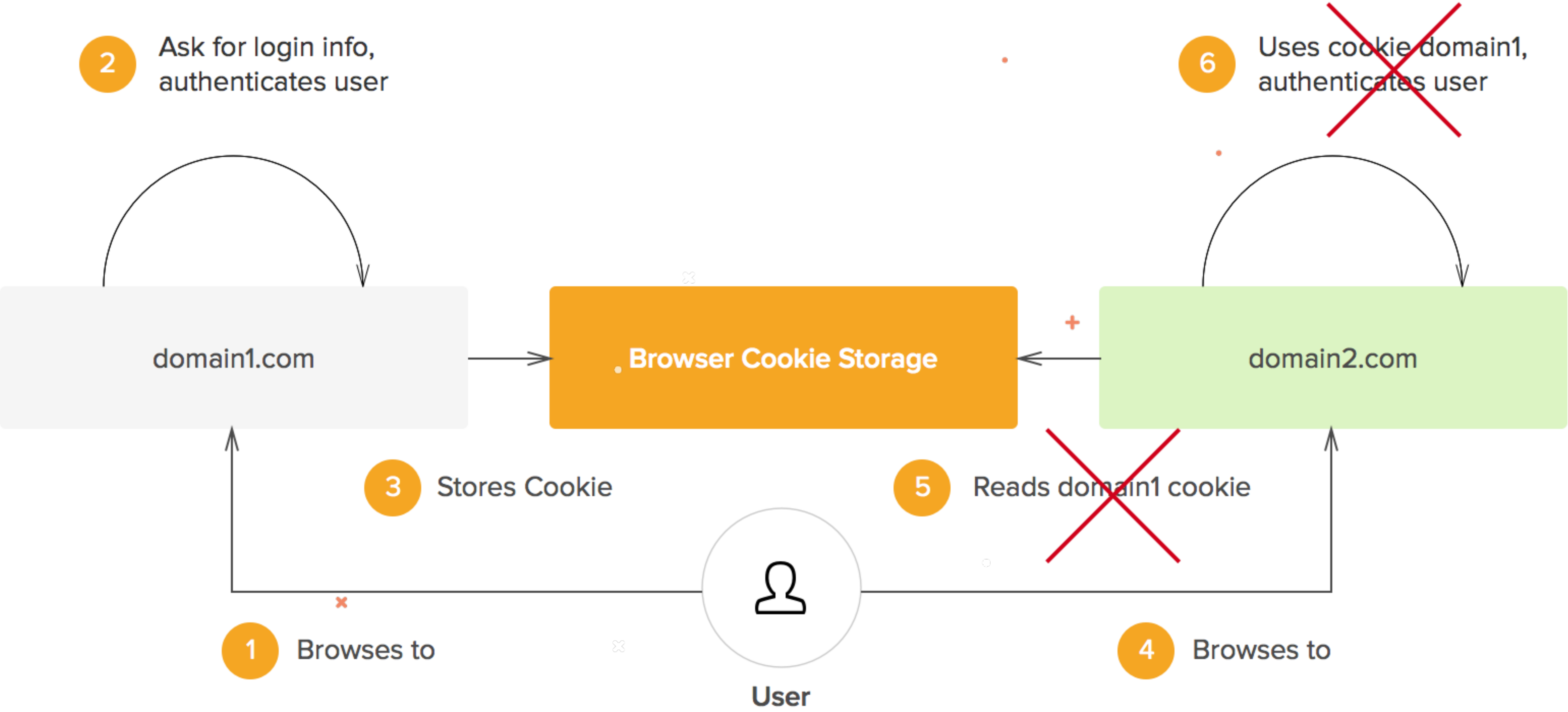
IAM

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

@itrwyss

Same-Origin Policy

IAM



2 Ask for login info, authenticates user
6 ~~Uses cookie domain1, authenticates user~~
domain1.com
Browser Cookie Storage
domain2.com
3 Stores Cookie
5 ~~Reads domain1 cookie~~
1 Browses to
4 Browses to
User

@itrwyss

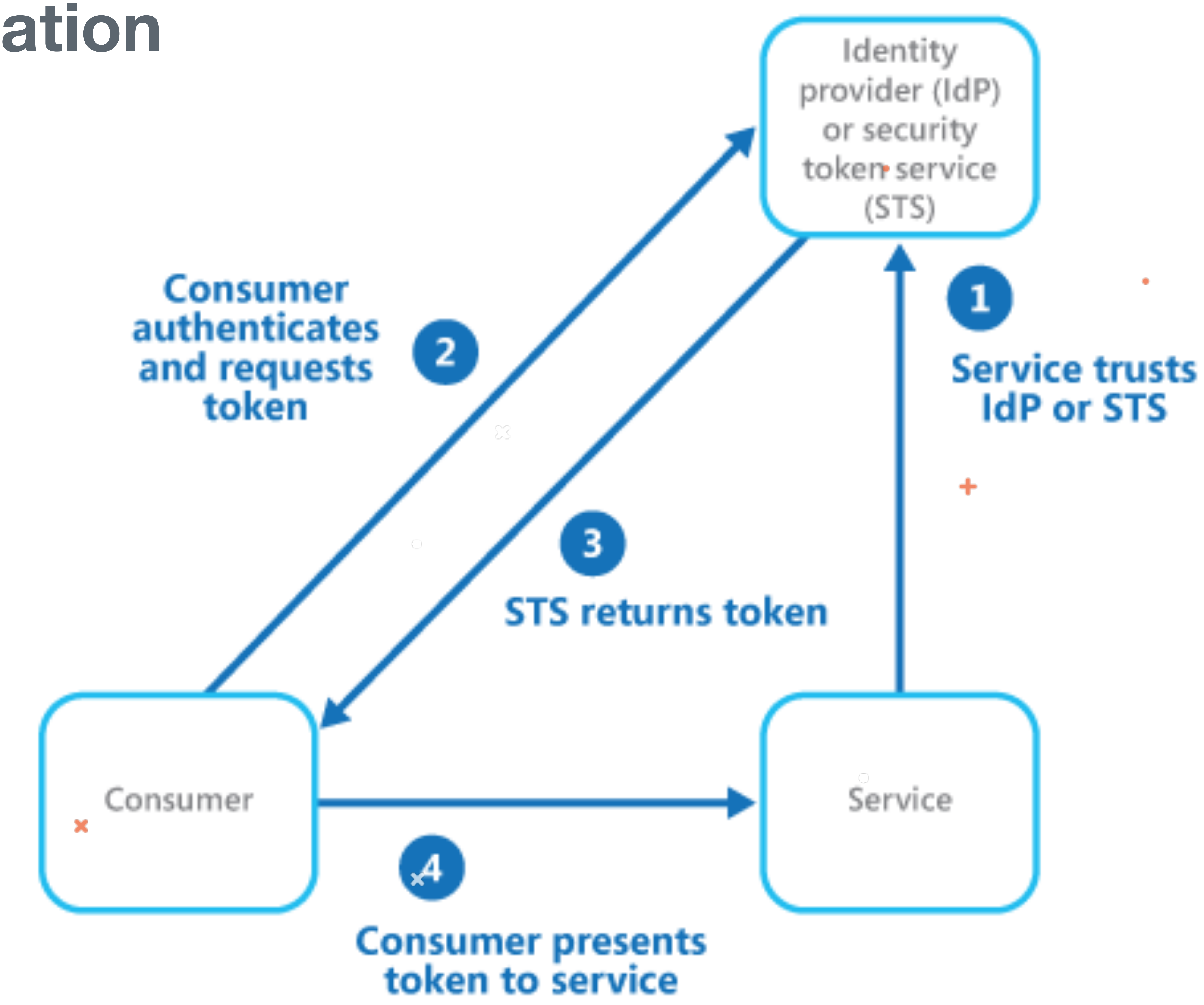
Identity Federation

IAM

- 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.

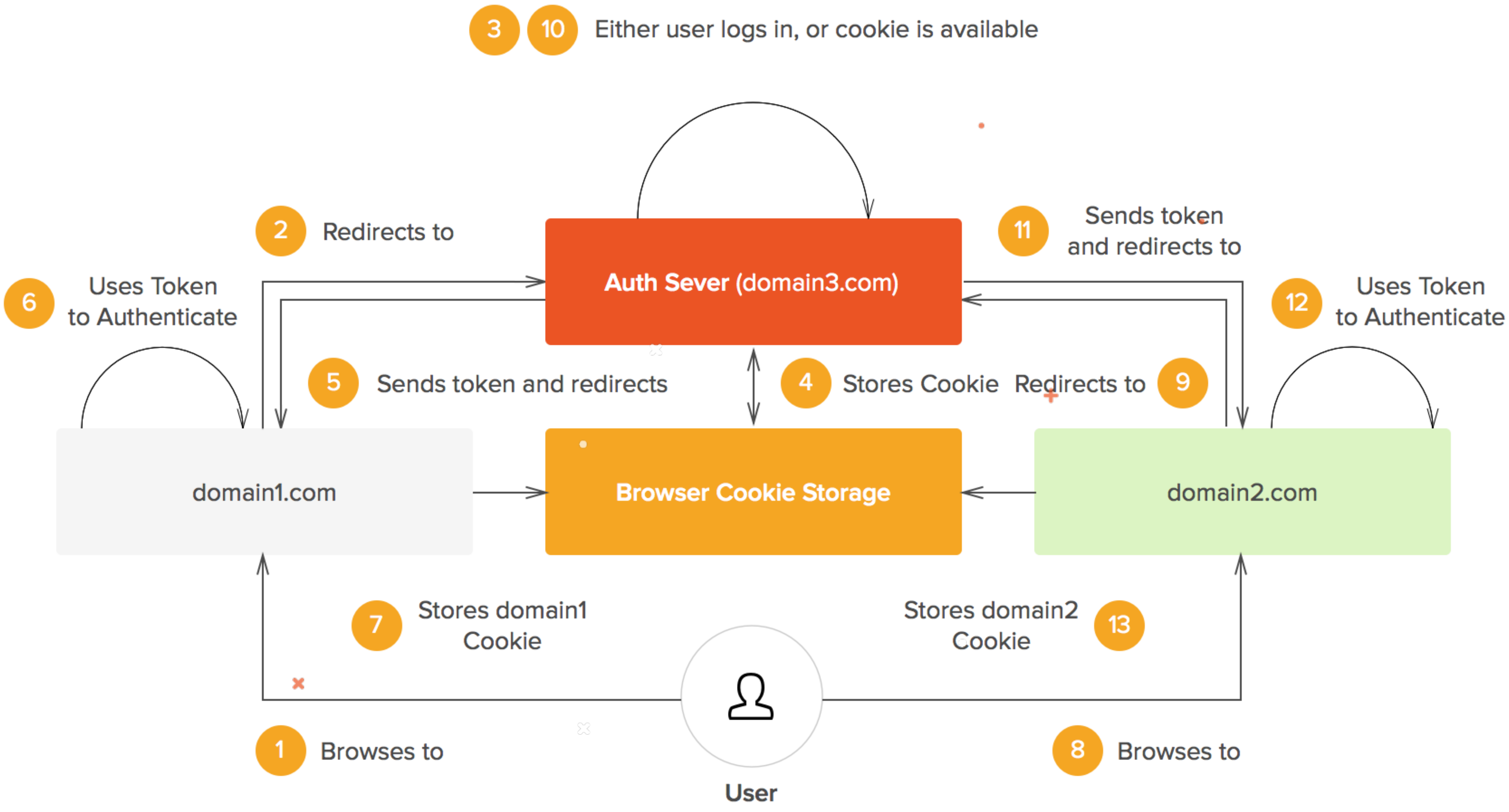
External Authorization Server

Identity Federation


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

@itrwyss

Login Related Domains



@itrwyss

Authentication

IAM

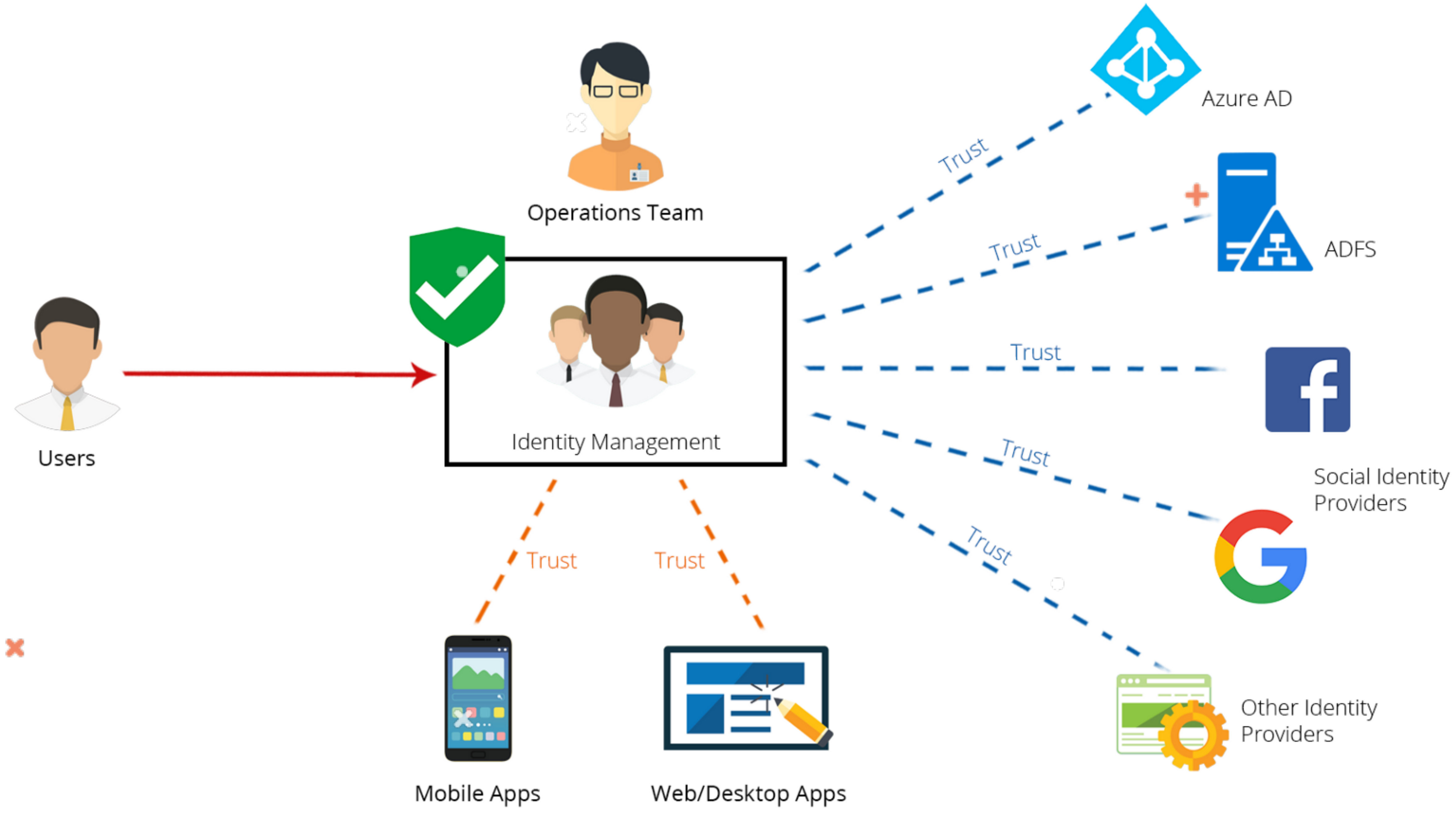
Ensuring that a given user is the user they identify as

- Single Sign-On (SSO)
- Multi-factor Authentication (MFA)
- Passwordless
- Federated Identity (Management)

Federated Identity (Management)

Authentication

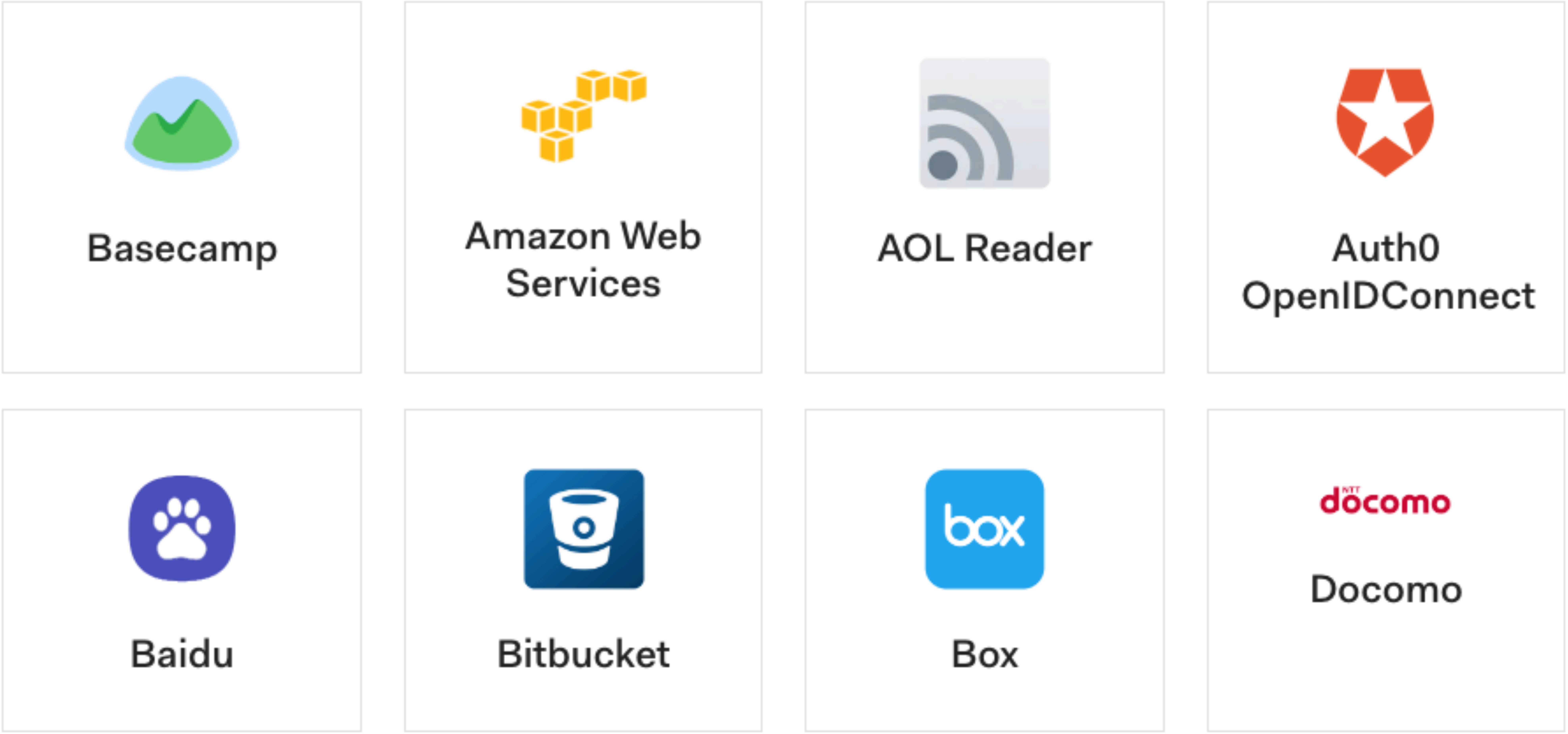
- Linking a person’s electronic identity and attributes, stored across multiple distinct identity management systems.



@itrwyss

Social Federated Identity

@itrwyss



Basecamp

Amazon Web Services

AOL Reader

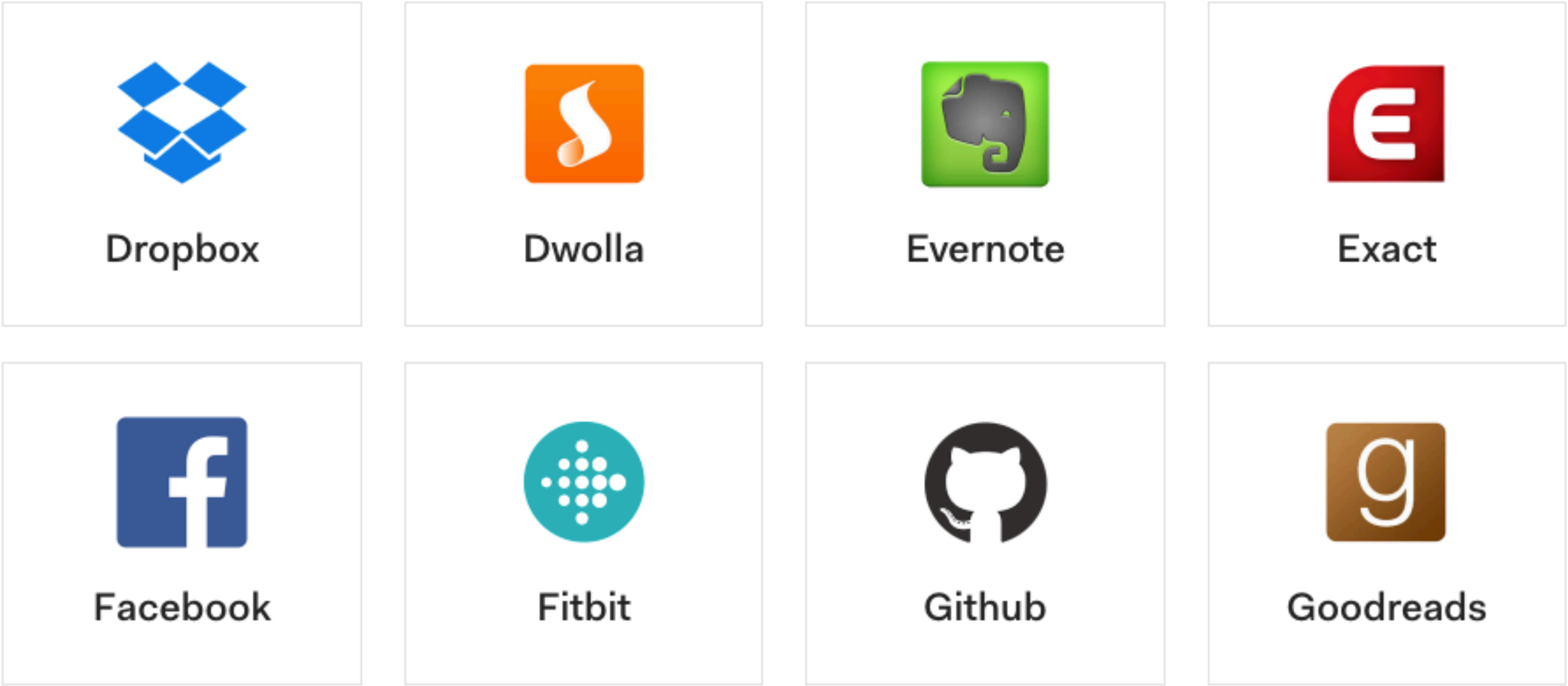
Auth0 OpenIDConnect

Baidu

Bitbucket

Box

Docomo



Dropbox

Dwolla

Evernote

Exact

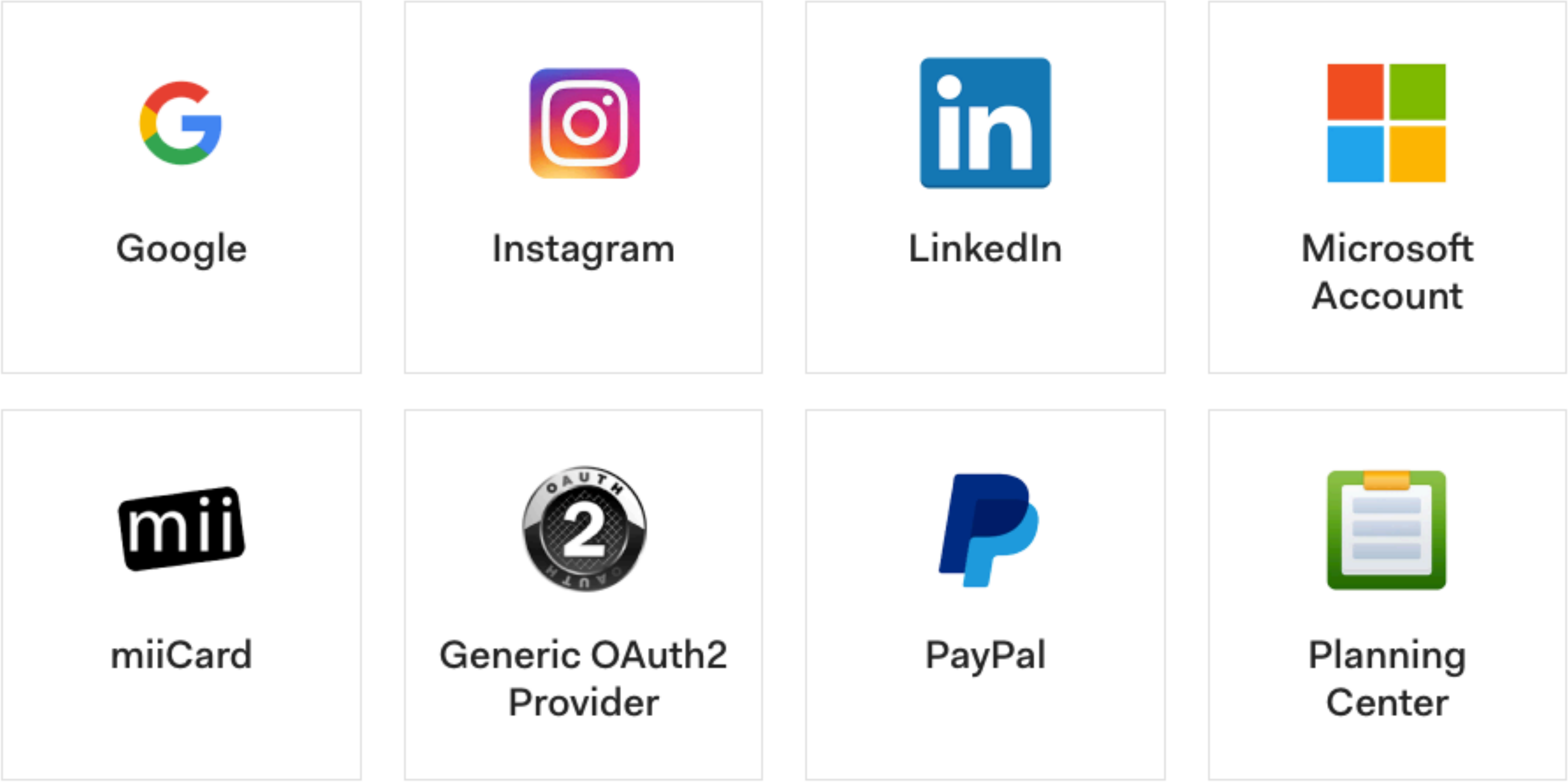
Facebook

Fitbit

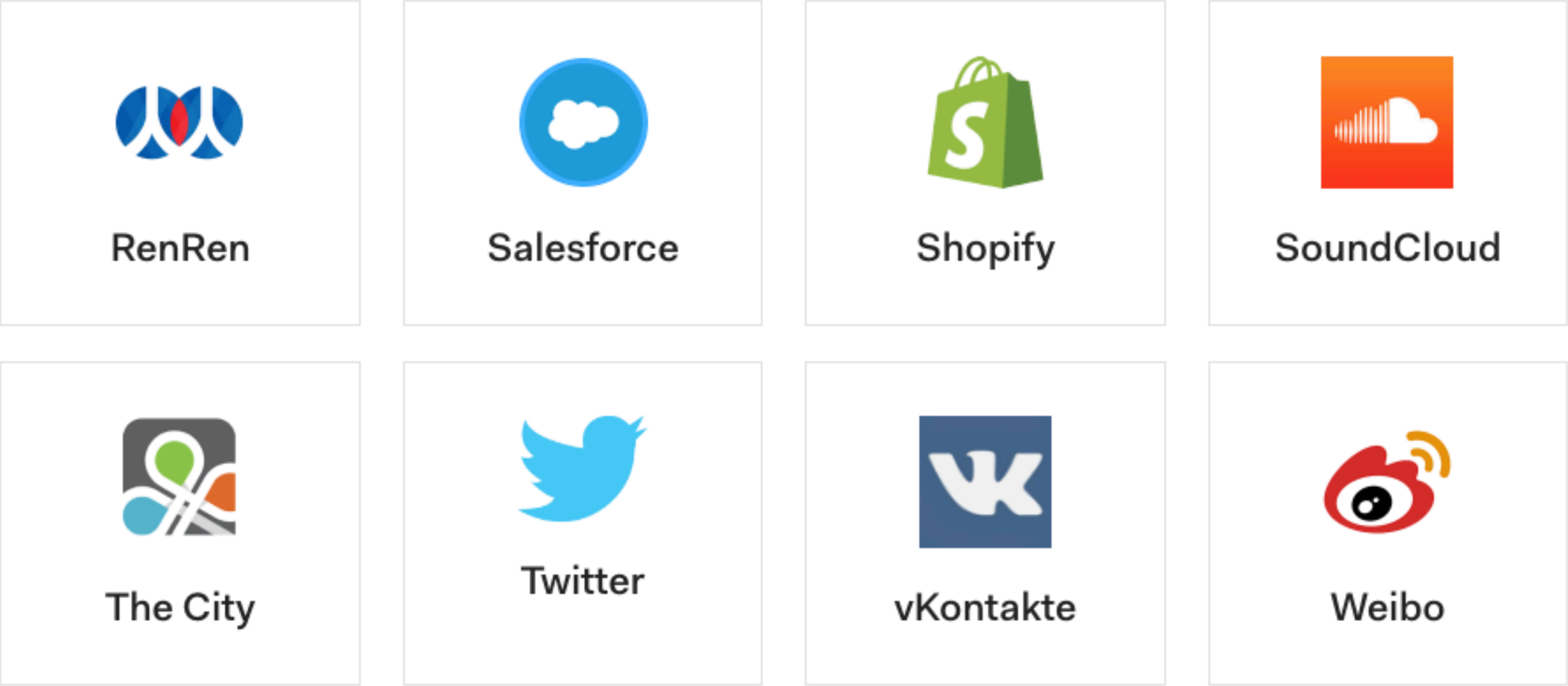
Github

Goodreads

@itrwyss


Google
Instagram
LinkedIn
Microsoft Account
miiCard
Generic OAuth2 Provider
PayPal
Planning Center

@itrwyss



RenRen

Salesforce

Shopify

SoundCloud

The City

Twitter

vKontakte

Weibo

@itrwyss

WordPress

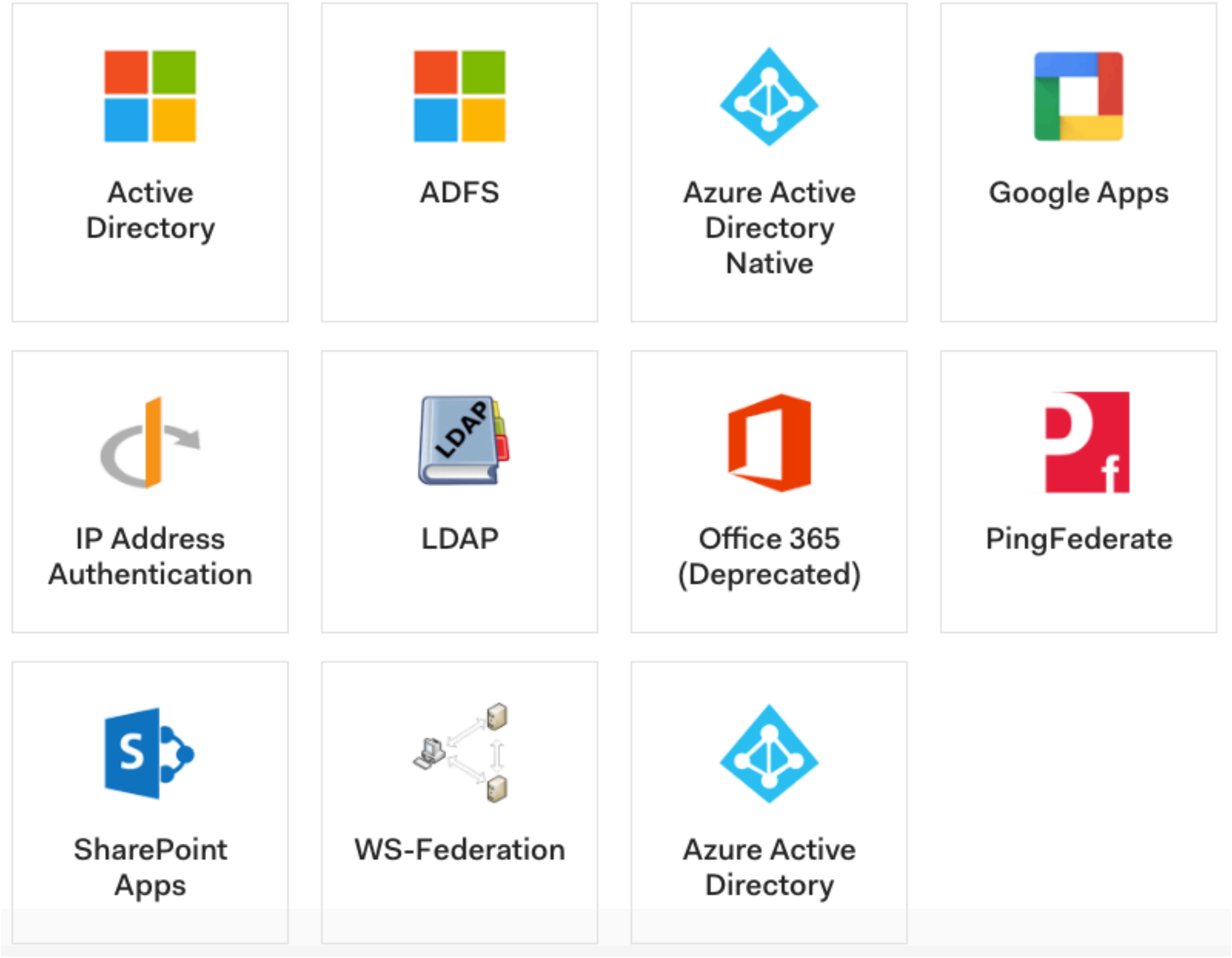
Yahoo!

Yammer

Yandex

Enterprise Federated Identity

@itrwyss


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

@itrwyss

bankID

Norwegian BankID

BankID

Swedish BankID

NEM ID

Danish NemID

Multi-Factor Authentication (MFA)

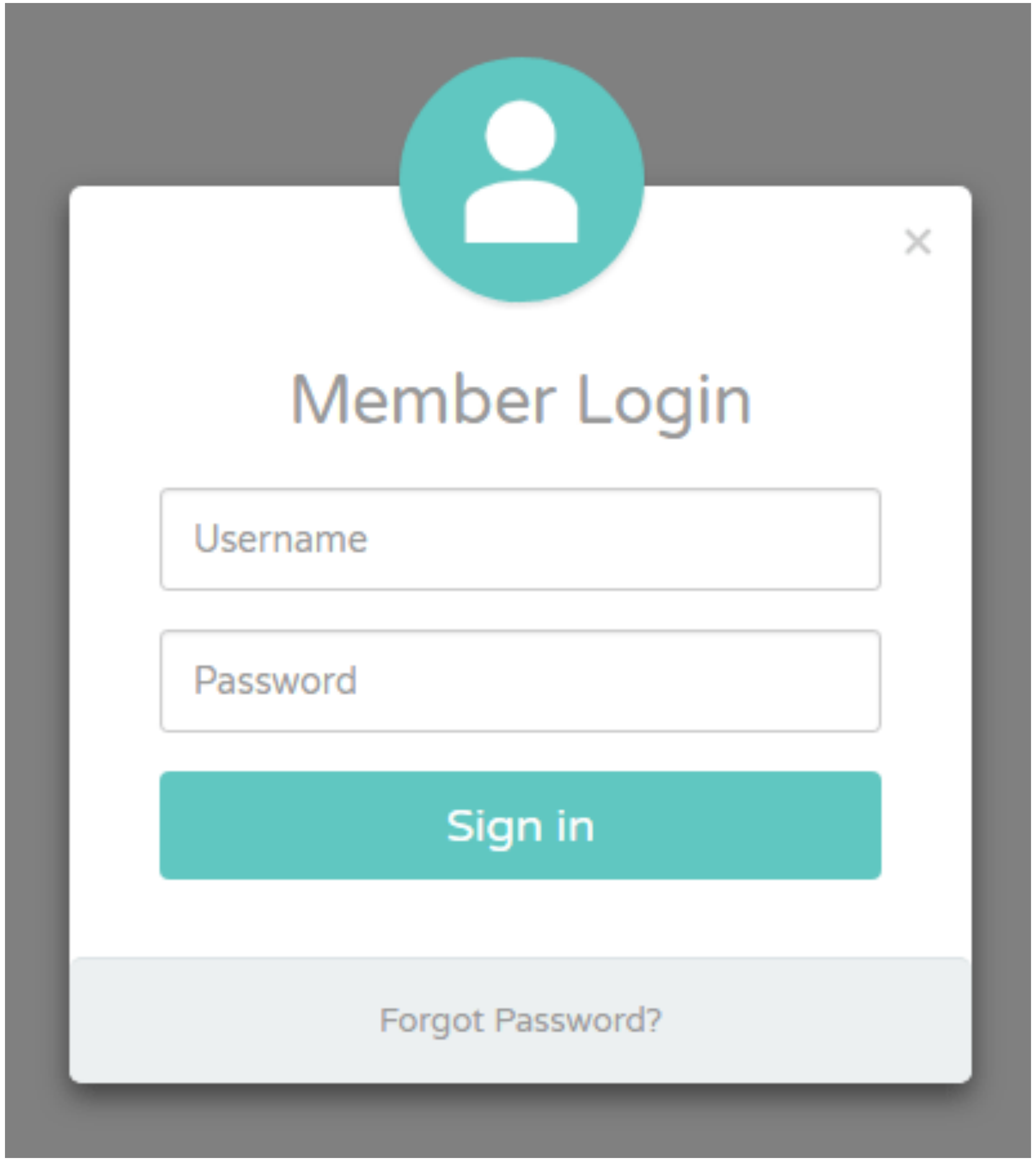
Authentication

Knowledge

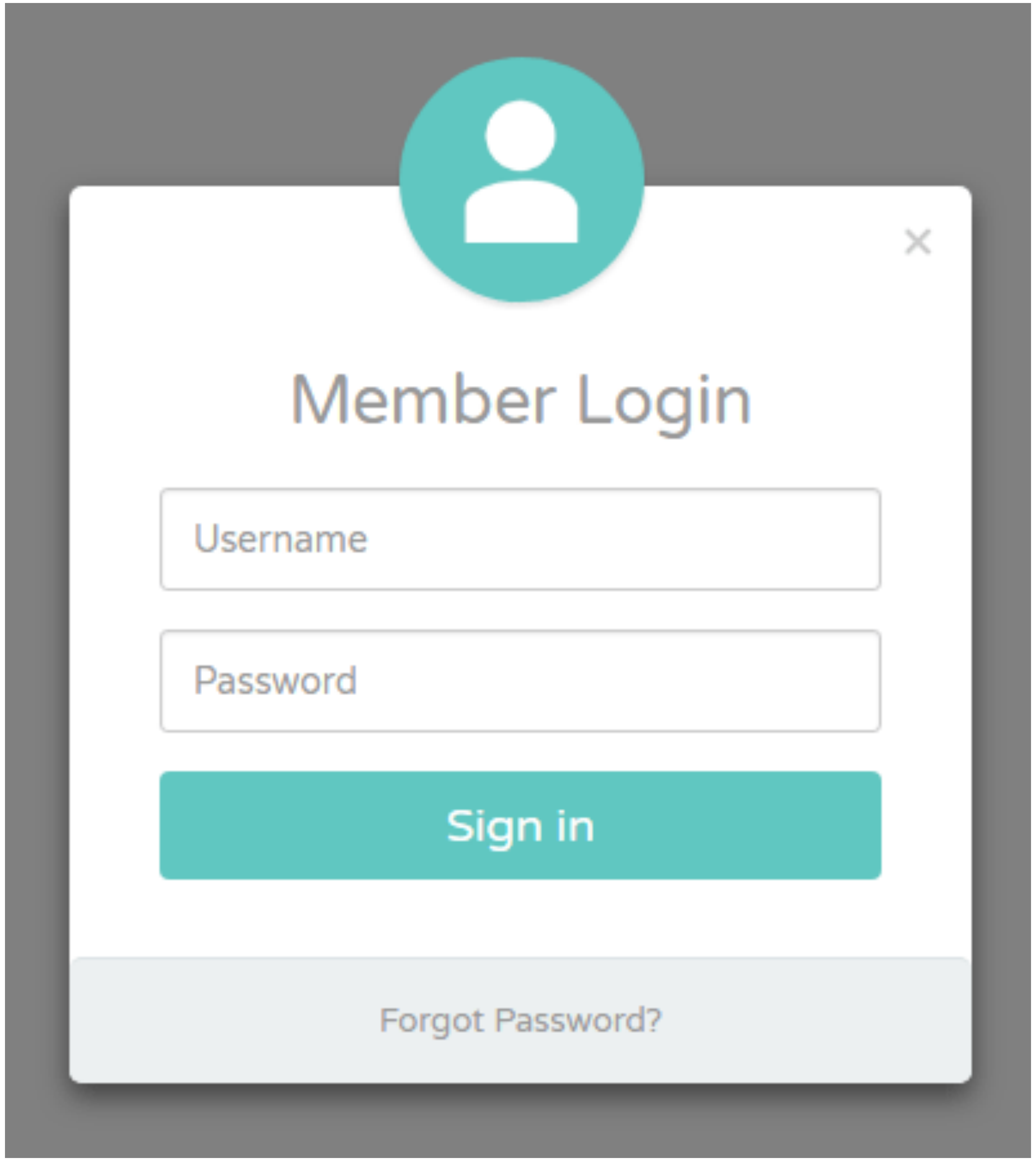
Possession

Biometric

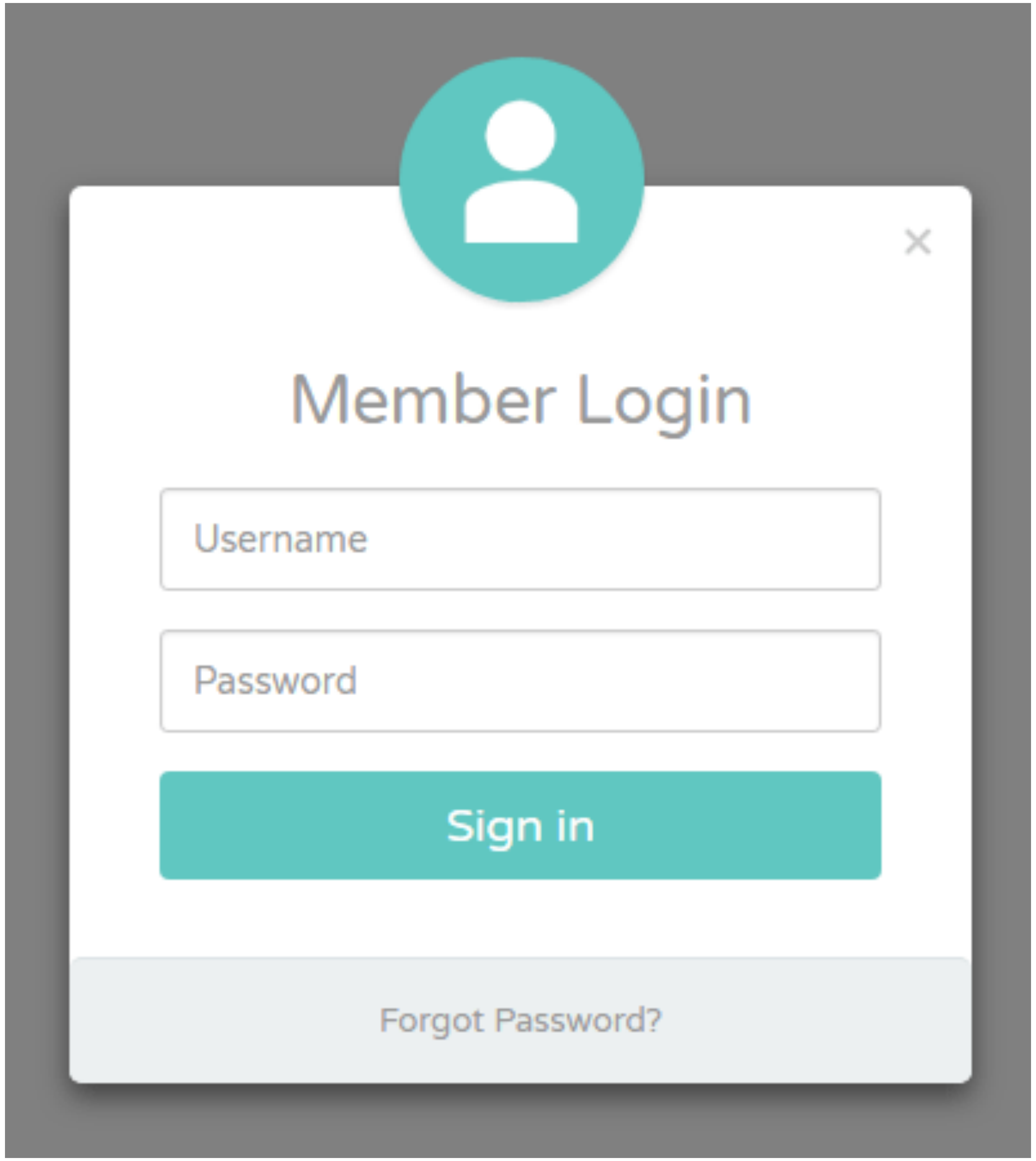
@itrwyss

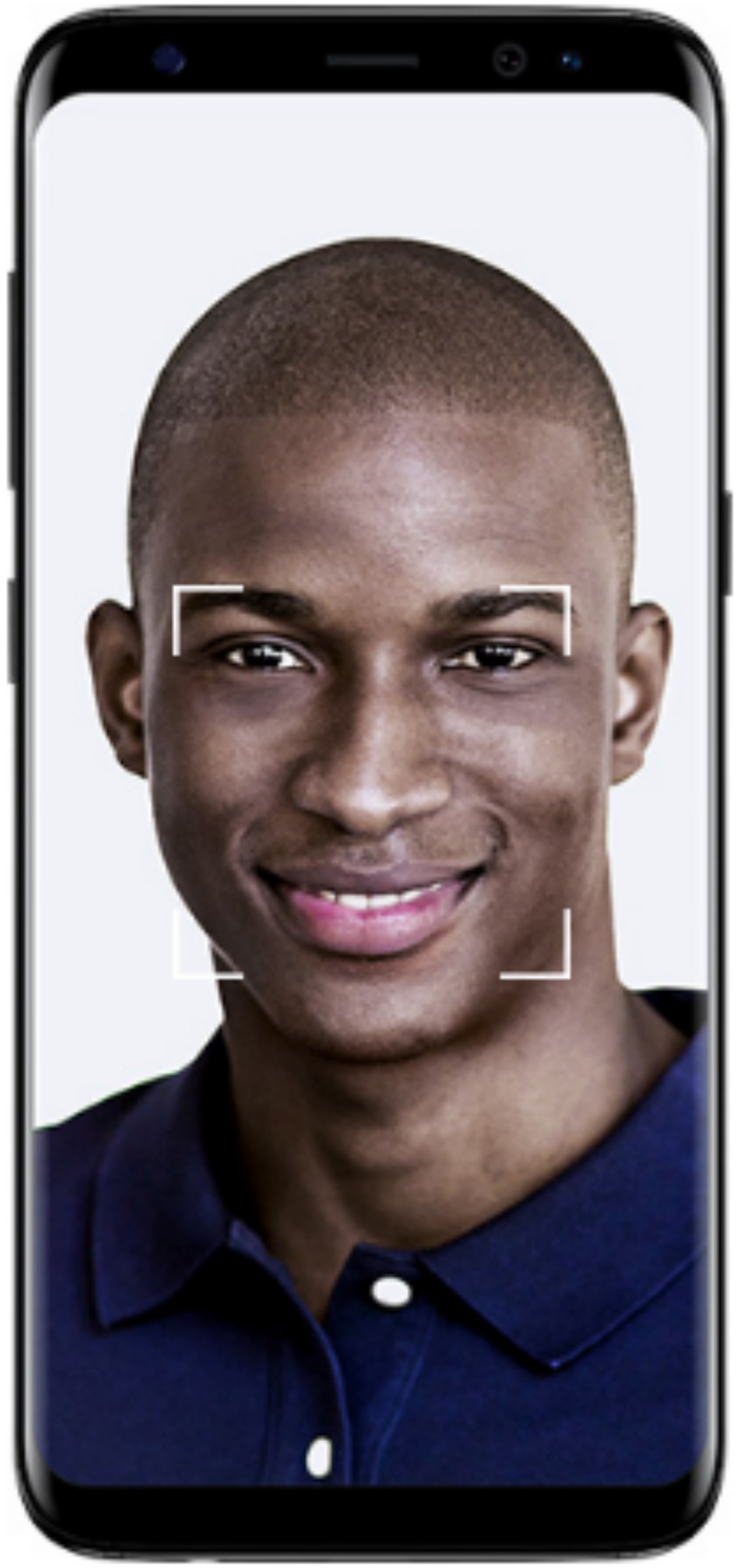


@itrwyss

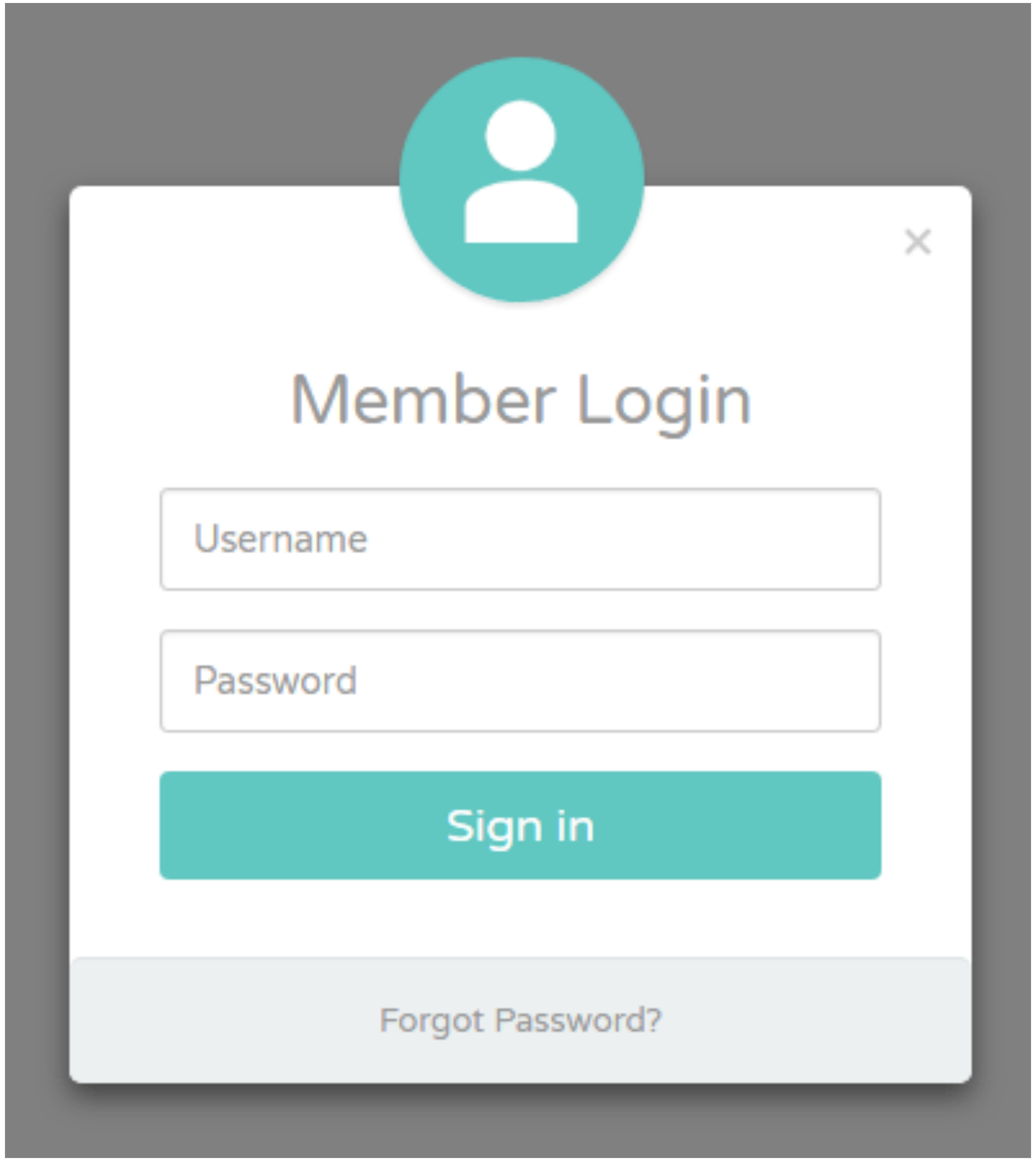

Member Login
Username
Password
Sign in
Forgot Password?

RSA
SecurID®
159 759.
Secured by RSA





@itrwyss



Member Login

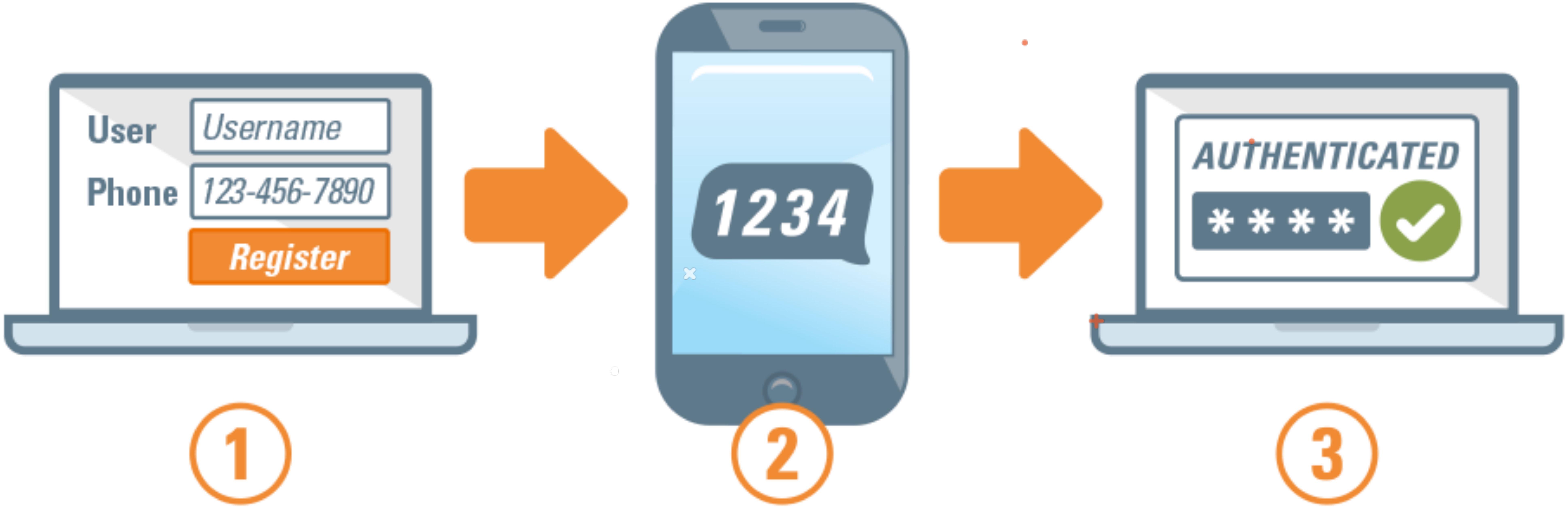
@itrwyss

Multi-Factor Authentication (MFA)

Authentication

Multi-Factor Authentication (MFA)

Authentication

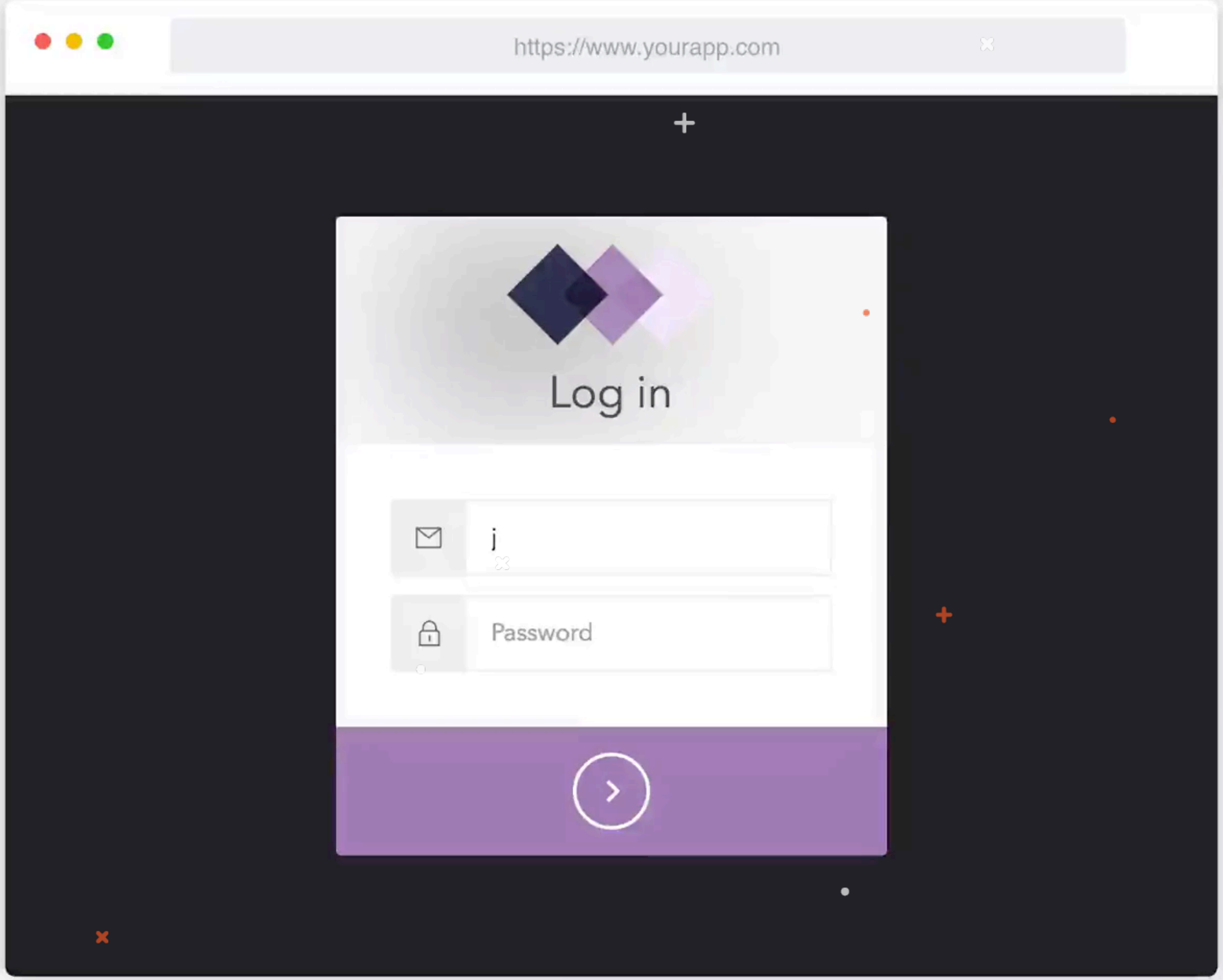


User logs into an account using their primary password

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

@itrwyss



https://www.yourapp.com

Log in

j

Password

@itrwyss

Biometrics

MFA

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

Biometrics

MFA

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

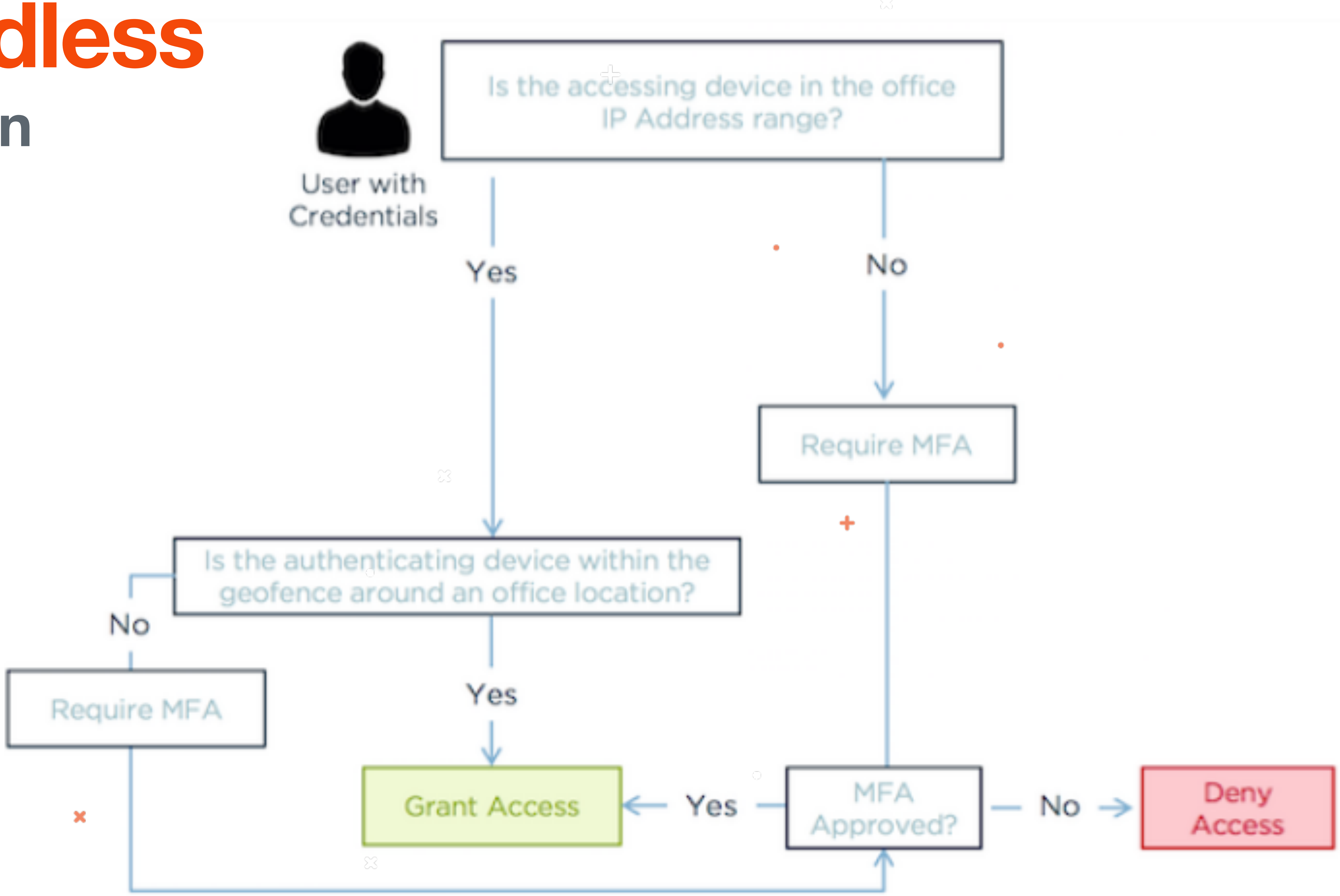
Passwordless

Authentication

- 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.

Passwordless

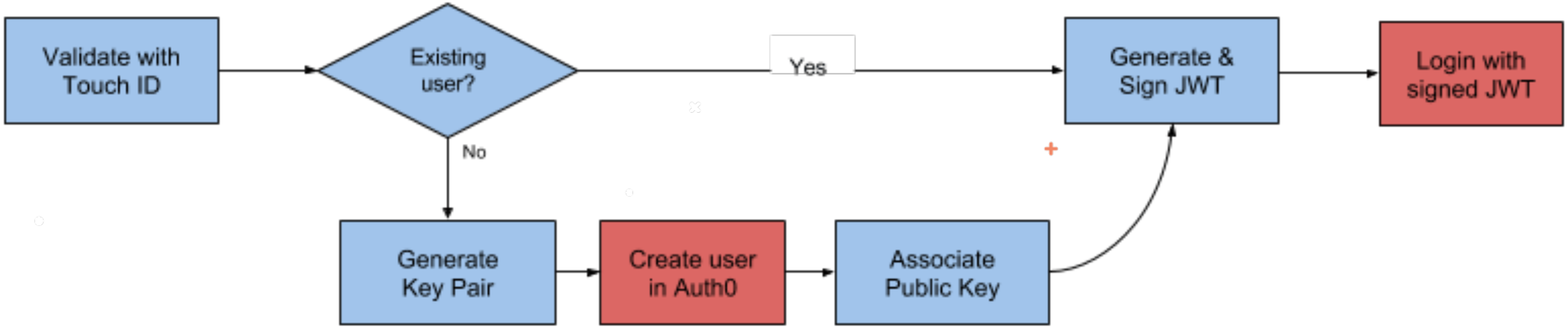
Authentication


User with Credentials
Is the accessing device in the office IP Address range?
Yes
No
Require MFA
Is the authenticating device within the geofence around an office location?
No
Yes
Require MFA
Grant Access
Yes
MFA Approved?
No
Deny Access

@itrwyss

Touch ID

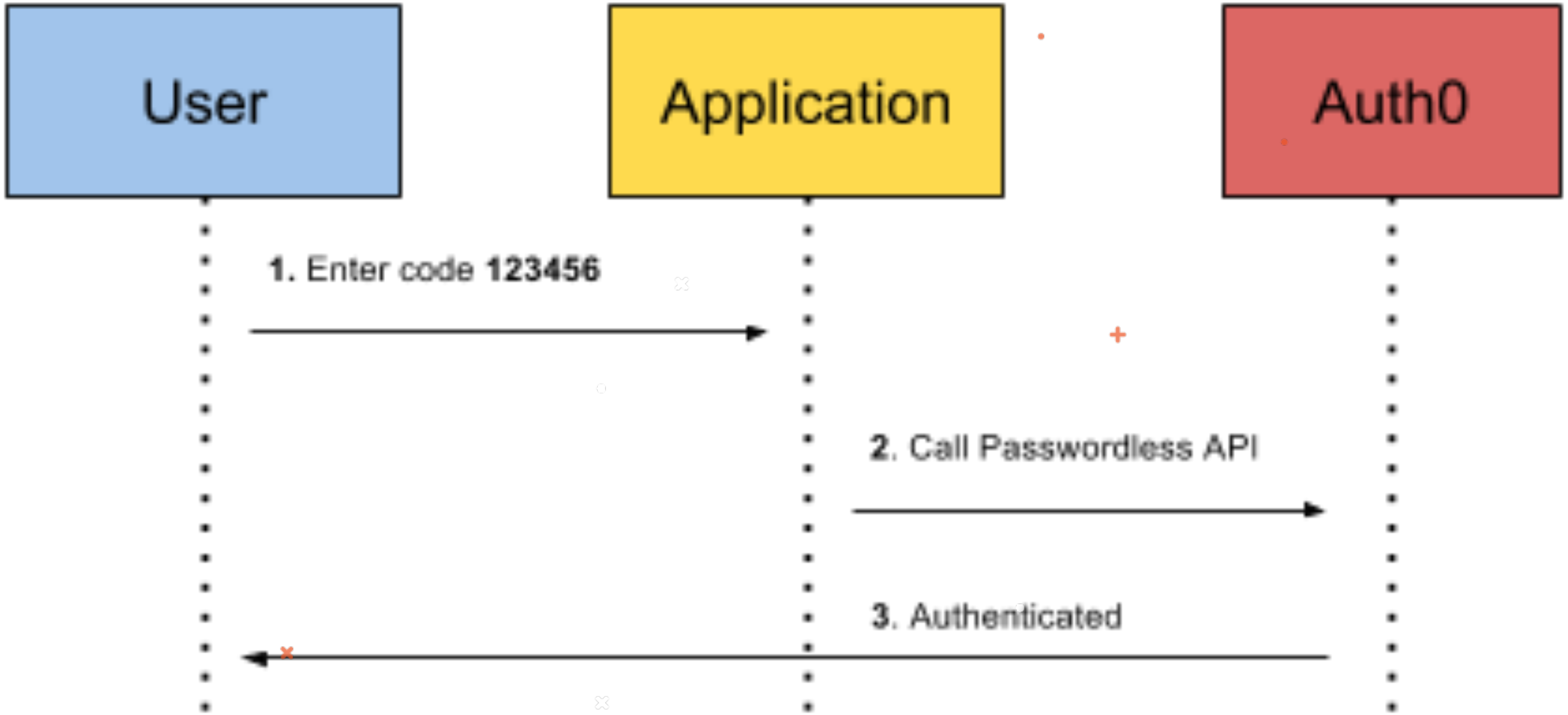
Passwordless



@itrwyss

SMS Code

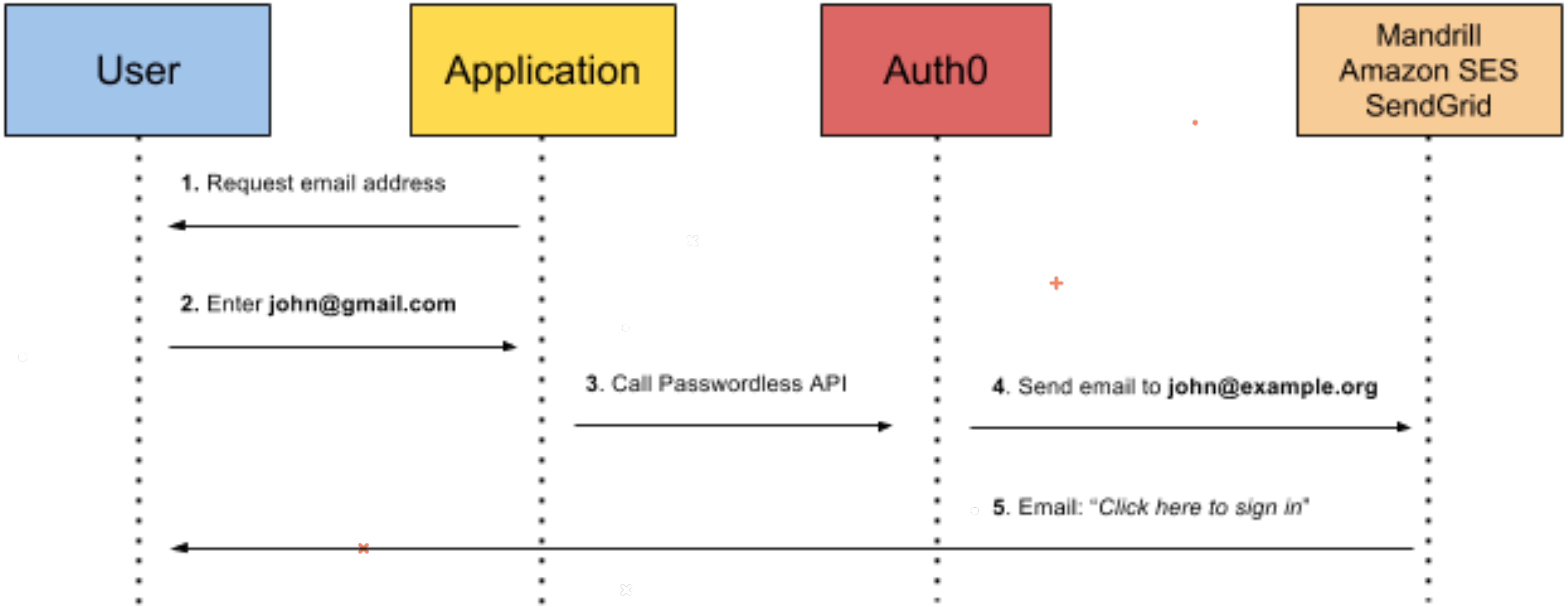
Passwordless



@itrwyss

Magic Link

Passwordless



User

Application

Auth0

Mandrill
Amazon SES
SendGrid

1. Request email address

2. Enter **john@gmail.com**

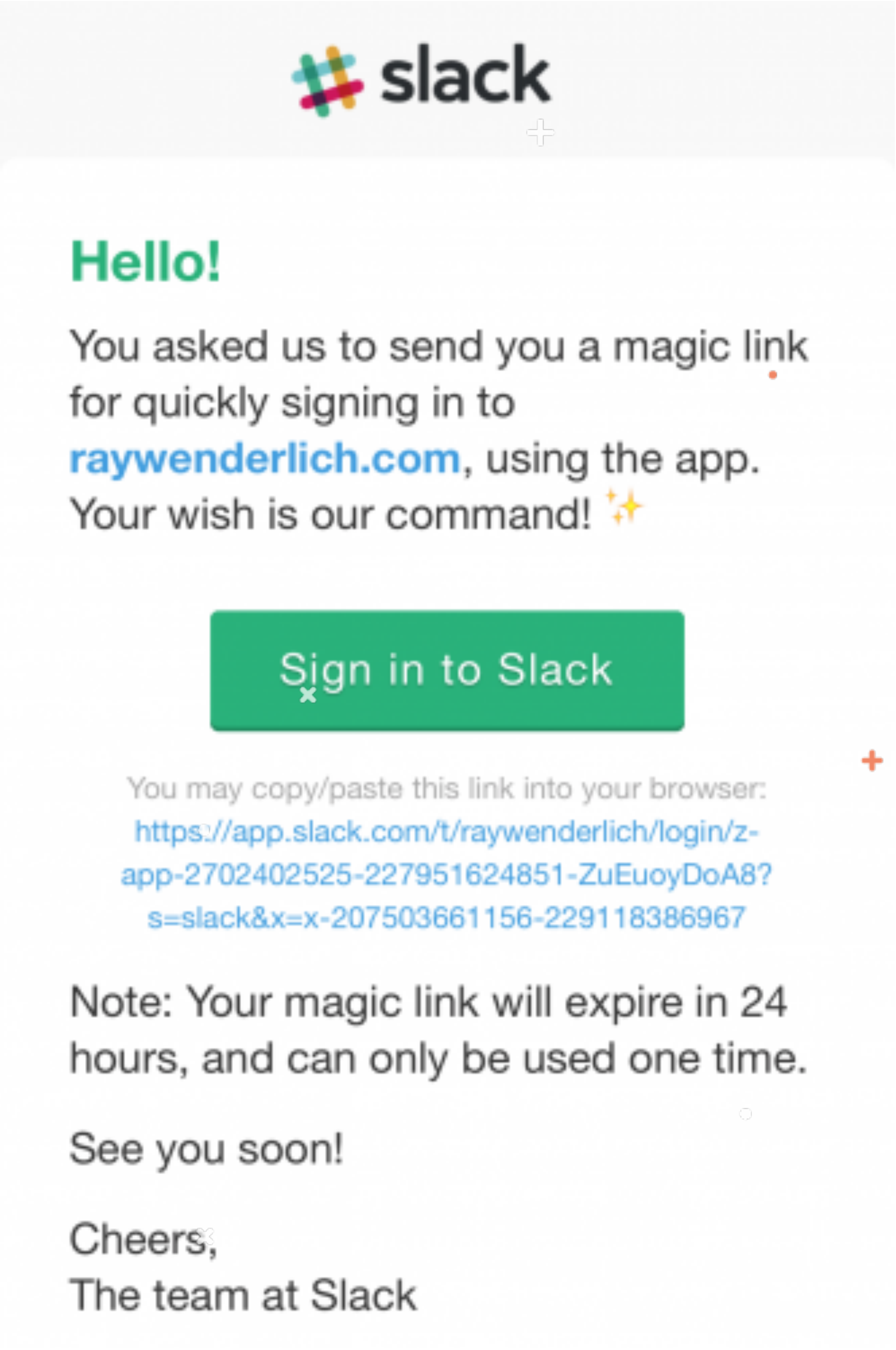
3. Call Passwordless API

4. Send email to **john@example.org**

5. Email: "*Click here to sign in*"

@itrwyss

@itrwyss



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

How to have a successful Identity Management Project

@itrwyss

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

@itrwyss

1. How will user accounts be created?

@itrwyss

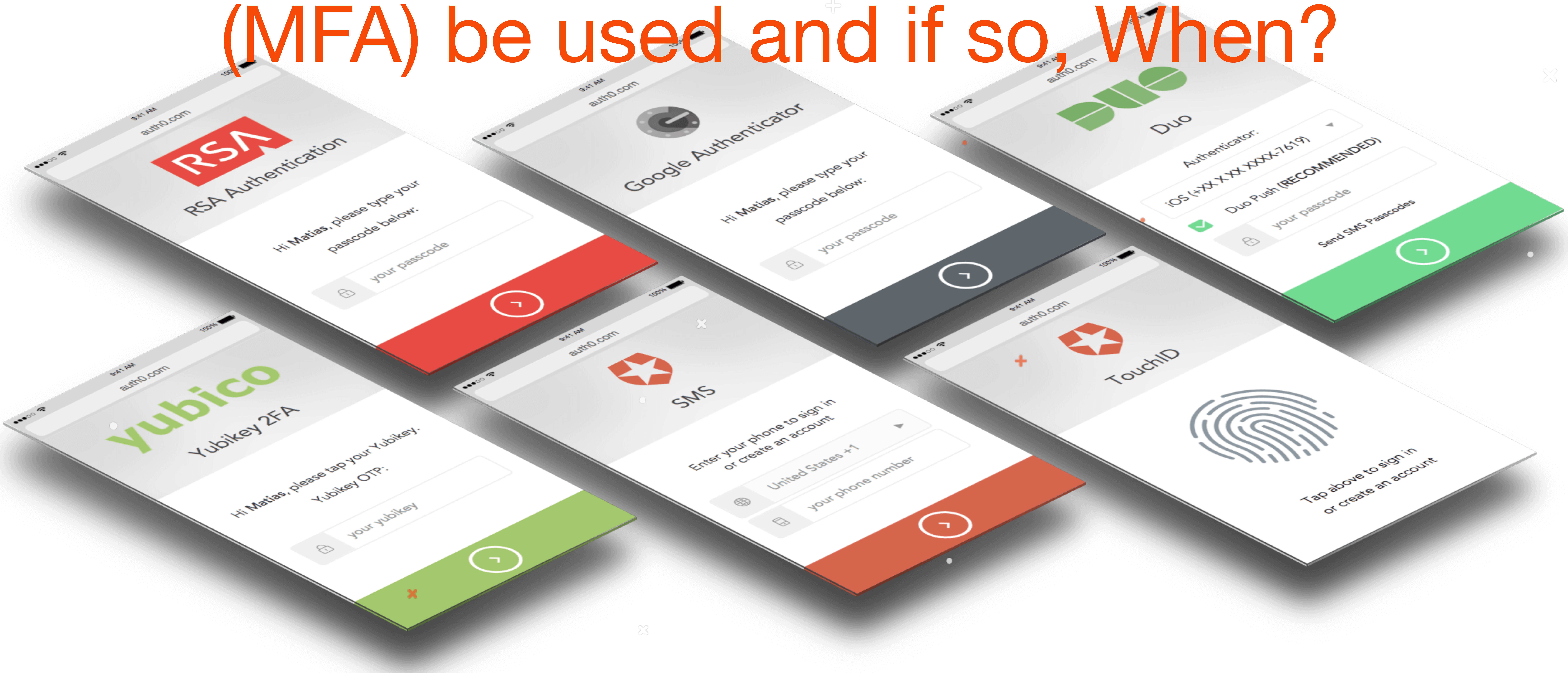
2. Will user profiles need to be synchronized?

@itrwyss

3. Username uniqueness

4. How will users Log In?

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



9:41 AM
auth0.com
RSA
RSA Authentication
Hi **Matias**, please type your passcode below:
your passcode

9:41 AM
auth0.com
Google Authenticator
Hi **Matias**, please type your passcode below:
your passcode

9:41 AM
auth0.com
Duo
Authenticator:
iOS (+XX X-XX-XXXX-7619)
Duo Push (RECOMMENDED)
your passcode
Send SMS Passcodes

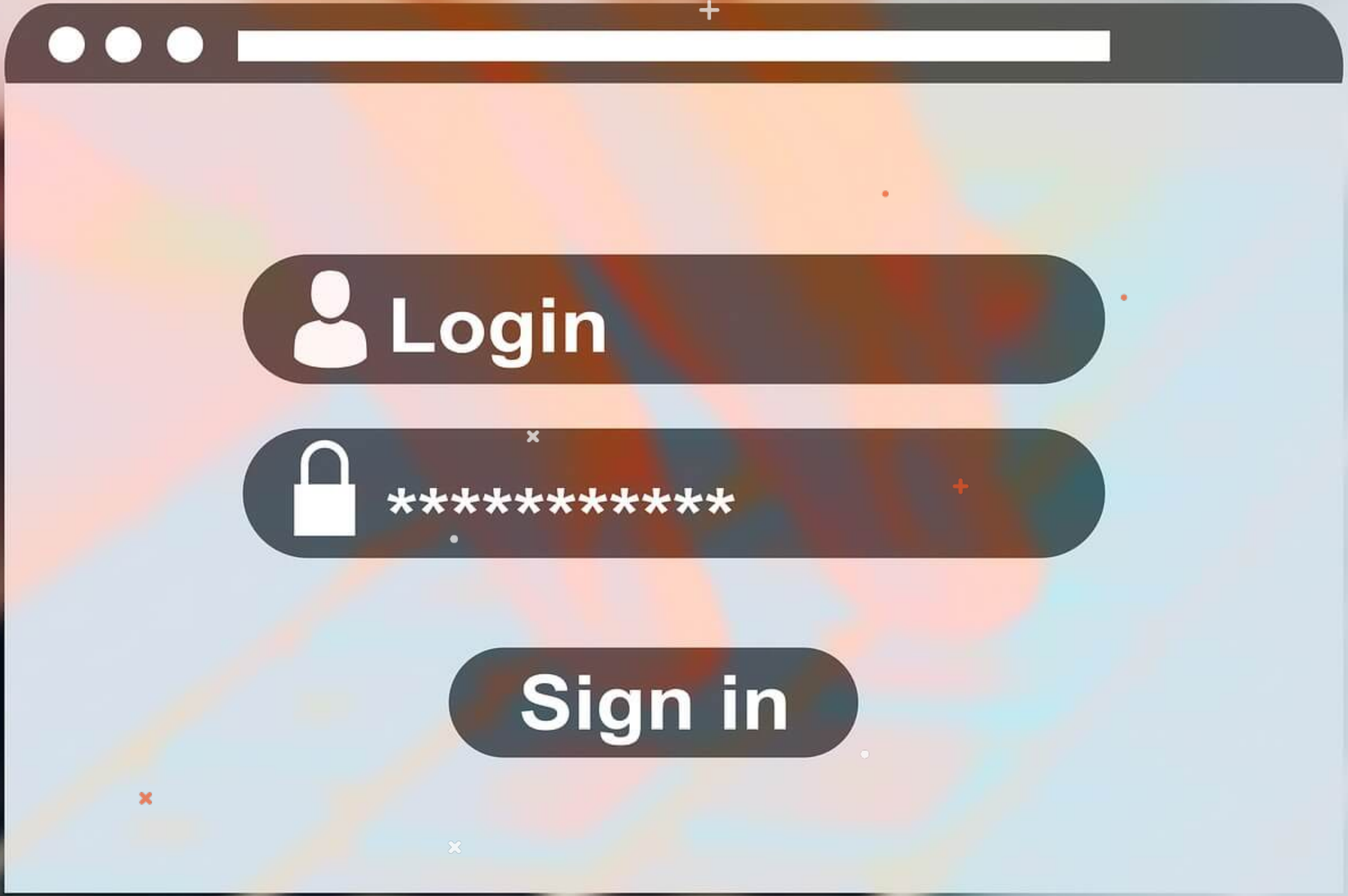
9:41 AM
auth0.com
yubico
Yubikey 2FA
Hi **Matias**, please tap your Yubikey.
Yubikey OTP:
your yubikey

9:41 AM
auth0.com
SMS
Enter your phone to sign in
or create an account
United States +1
your phone number

9:41 AM
auth0.com
TouchID
Tap above to sign in
or create an account

@itrwyss

6. Is single Sing-On needed?



@itrwyss

7. What devices will be used?

@itrwyss

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

9. How will browser configuration influence Sessions?

@itrwyss

10. Session Timeouts

@itrwyss

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

@itrwyss

12. Password Reset

13. Blocked Users

HARD HATS, HIGH VISIBILITY VESTS and SAFETY SHOES
MUST BE WORN ON THE WHARF AREA
WARNING
SECURITY REGULATED PORT
NO UNAUTHORISED ACCESS
Under the
Maritime Transport and Offshore Facilities Security Act (2003)
Aussie born and bred
PORT NOTICE
NO ENTRY
AUTHORISED PERSONS ONLY
Trespassers will be prosecuted

@itrwyss

14. Anomaly Detection

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 have I Been Pwned.

15. Privacy/Compliance requirements

Yale
Yale
Professional Standards Comm
The Professional Standards Co
The PSC comprises:
(a) a Member of the Institute ap
circumstances, is to be a mem
(b) between five and eleven other
the overall aim that there shoul
background and those with pro
body of knowledge from both an

@itrwyss

16. Audit Logs

@itrwyss

17. Consider how Identity Information might change over time

@itrwyss

Identity as a Service
IDaaS

@itrwyss

Identity as a Service

IDaaS

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

Popular Clouds

IDaaS

Azure Active Directory

ORACLE®
IDENTITY MANAGEMENT

Firebase
Authentication

amazon
web services

Auth0

@itrwyss

Other Popular

IDaaS

Other Providers

IDaaS

RSA
SecurID®
LogMeIn
Pro²
CROSSMATCH
The world identifies with us.
digitalPersona.
onelogin
Centrify®

@itrwyss

Other Providers

IDaaS

SailPoint

The Power of Identity™

INTERMEDIA AppID

ENTERPRISE

ForgeRock Identity Platform™

Identity Management

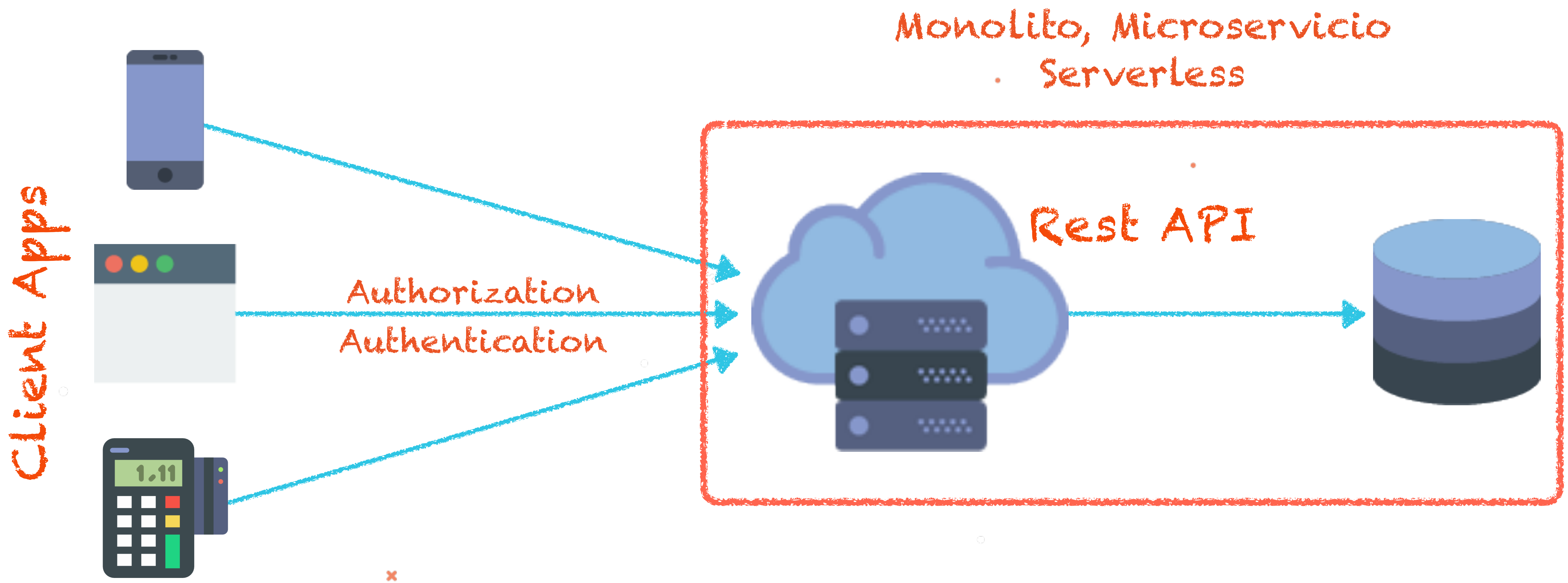
Based on the OpenIDM Project

miniOrange

Architecture Level

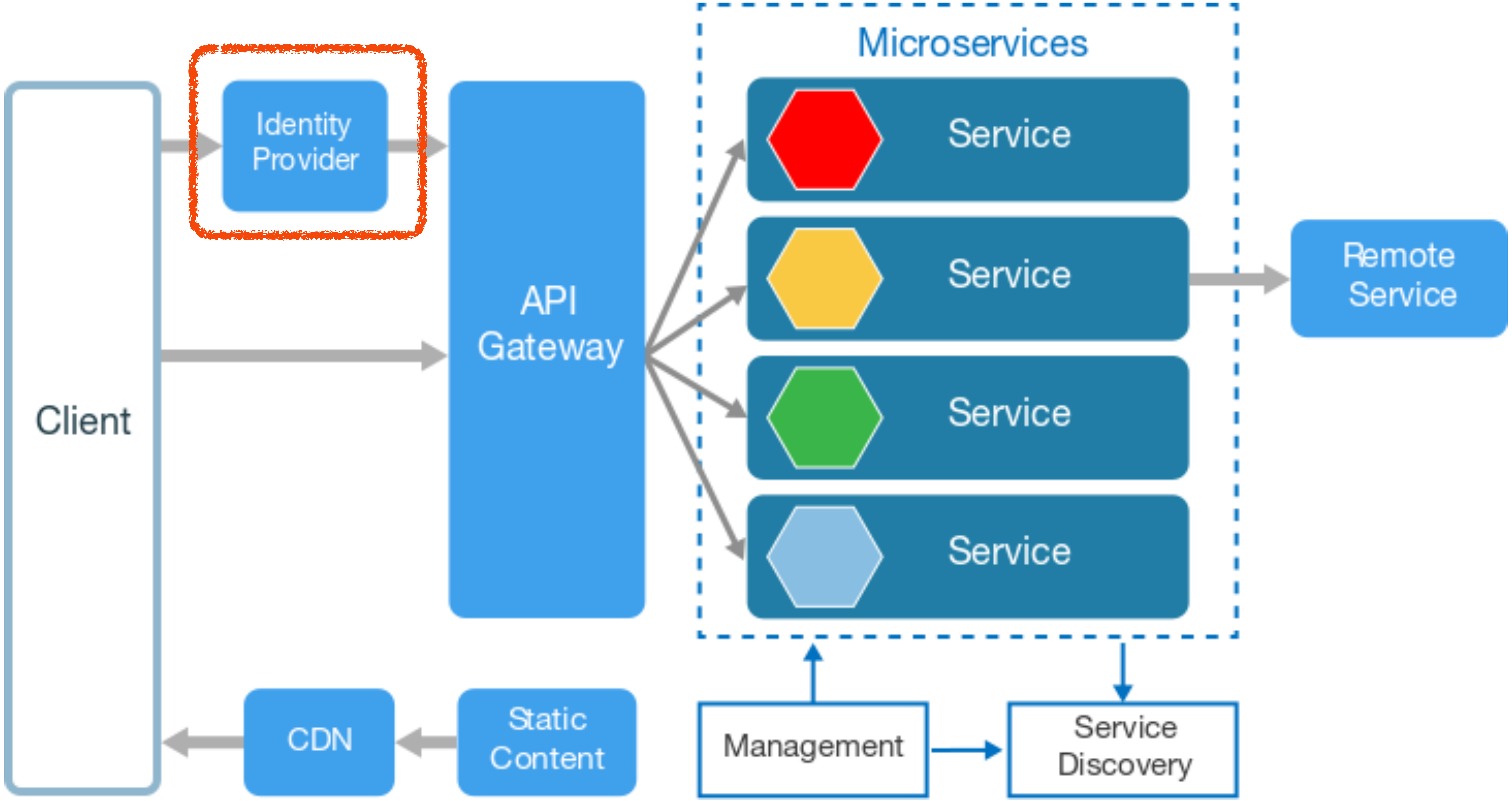
@itrwyss

Developing Rest APIs



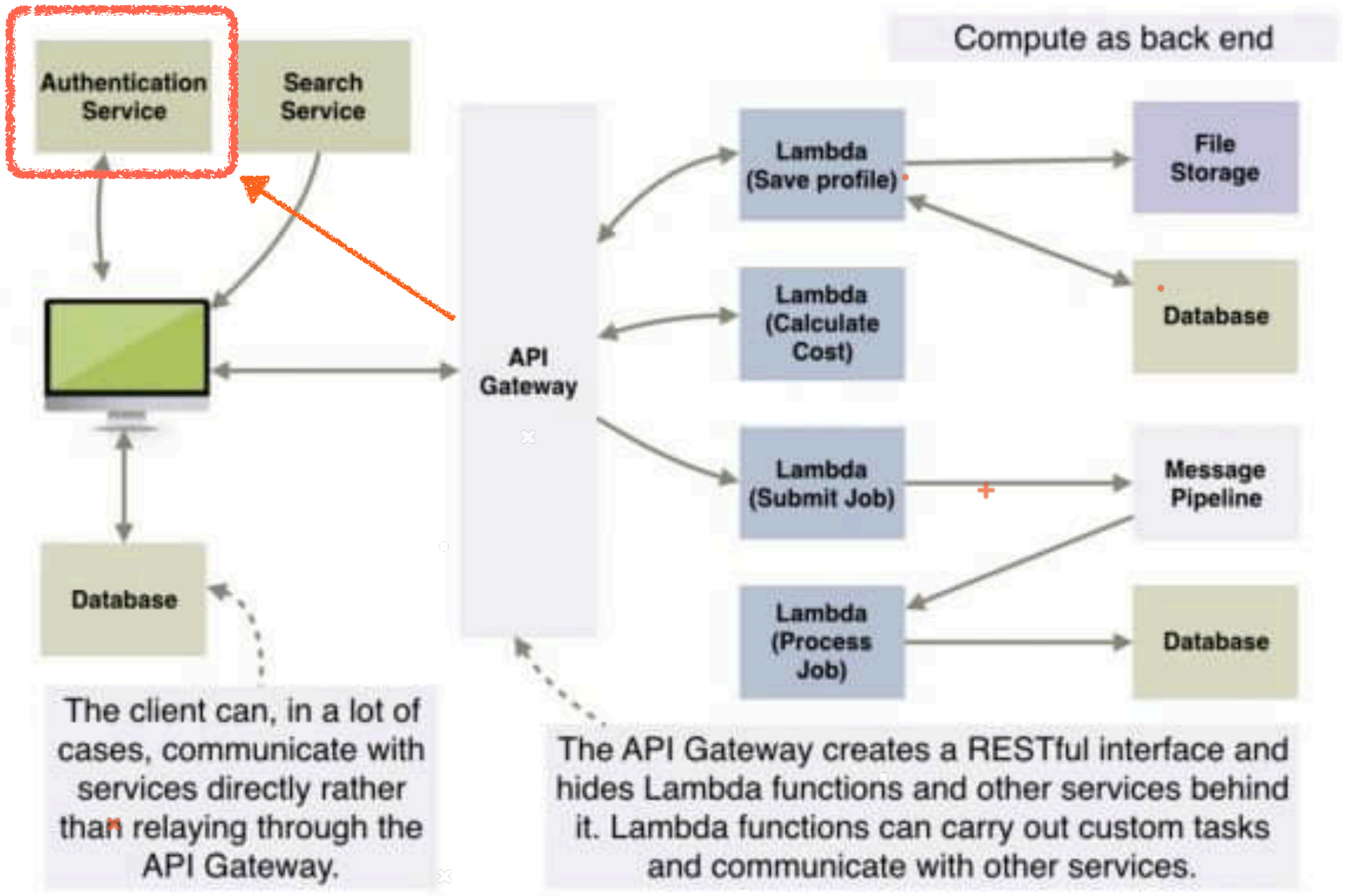
@itrwyss

Microservicios



@itrwyss

Serverless



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.

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

@itrwyss

Demo

@itrwyss

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

https://www.facebook.com/itrjwyss

@itrjwyss