A More Secure World for <Android/> Apps

DROIDCON 18

BOSTON

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 Developer Champion

Duke's Choice Award

2016 Winner

Java

AMBASSADOR

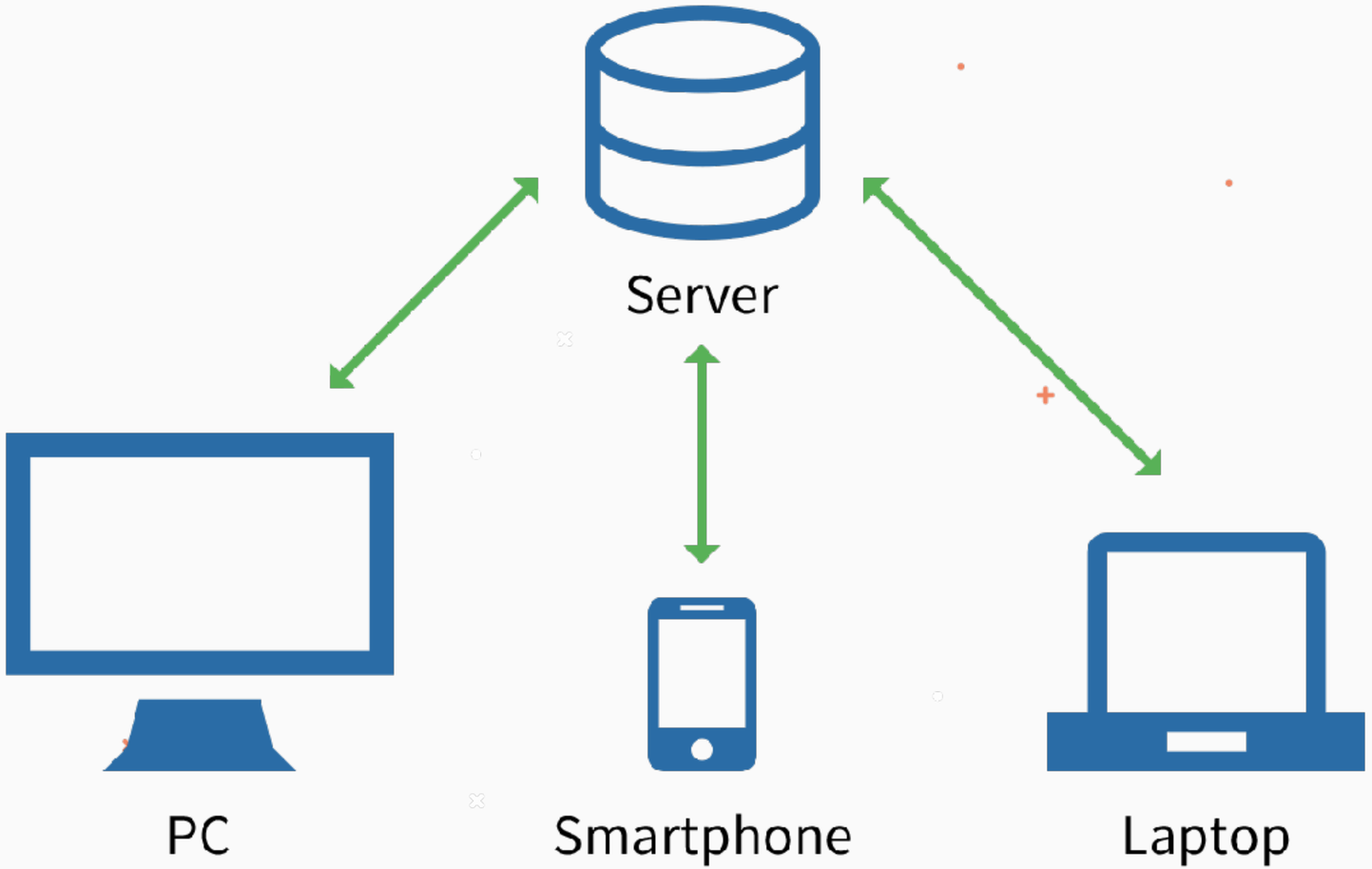
ORACLE Developer Champion

Devs +502

Comunidad Desarrolladores en Tecnologías < Google > en Guatemala

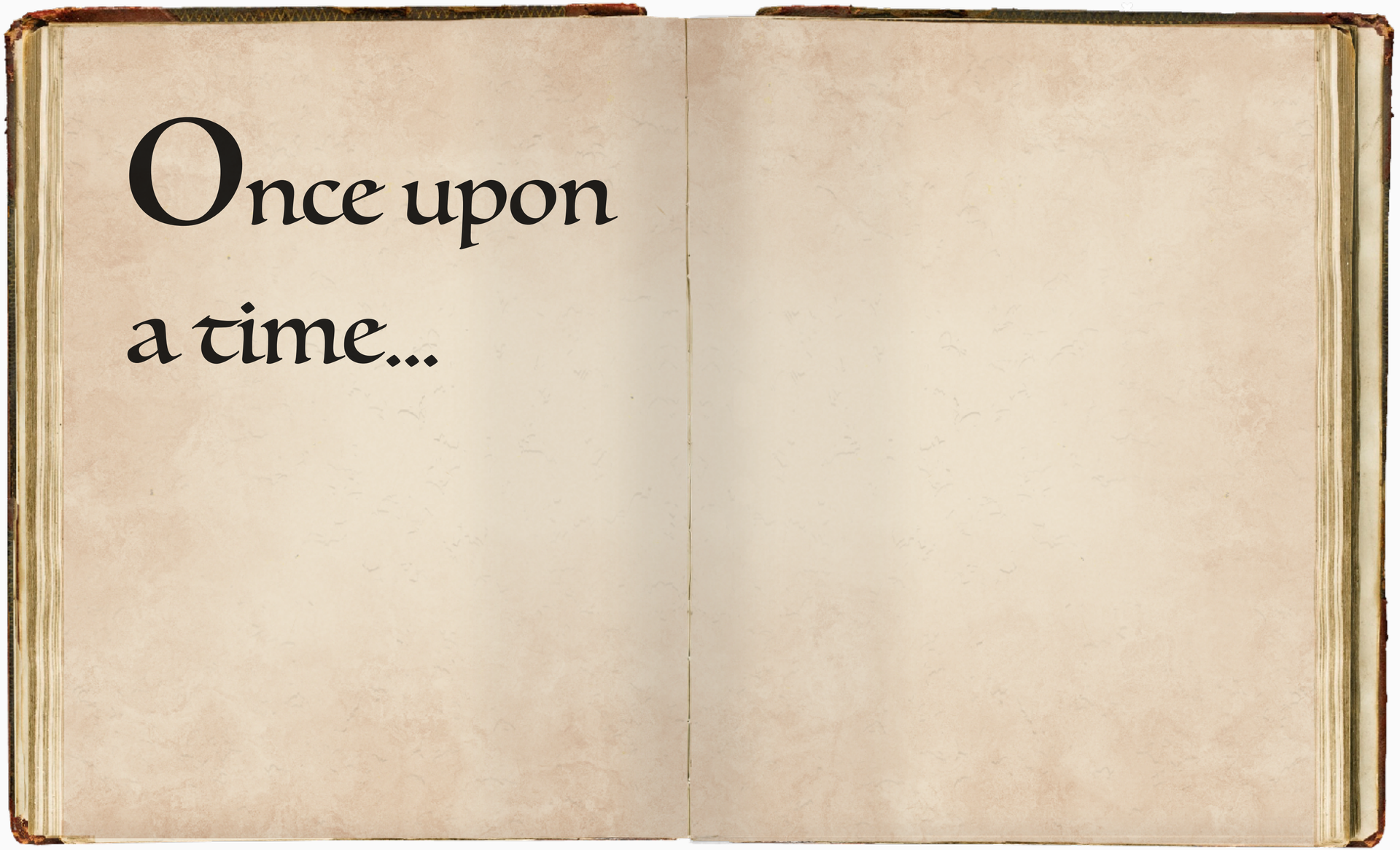
JDuchess Guatemala

Security is a Team Effort

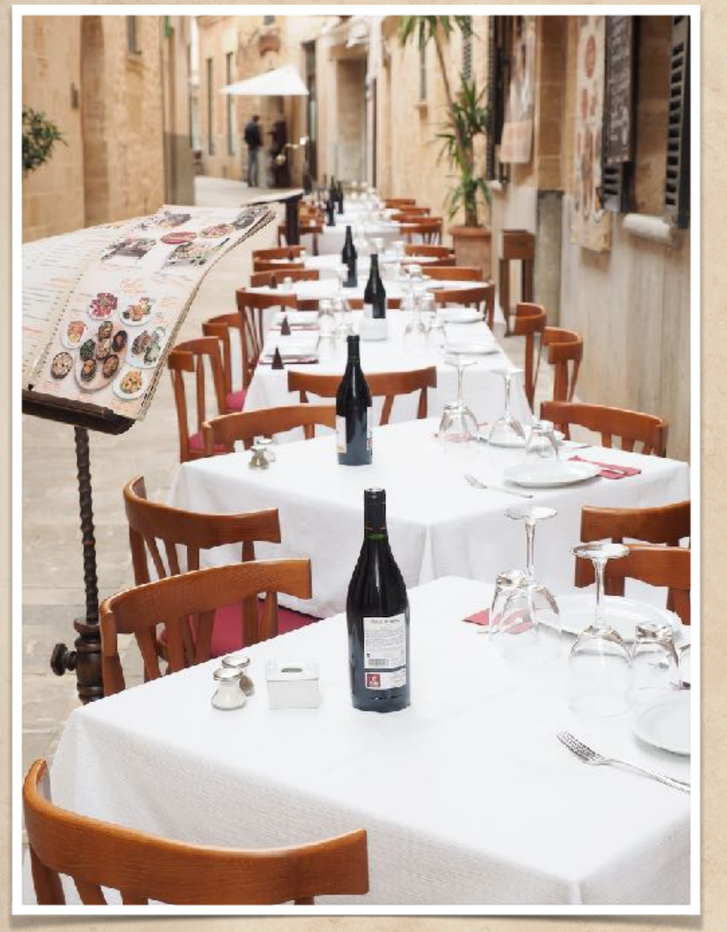


Free Hamburgers

ORACLE Developer Champion

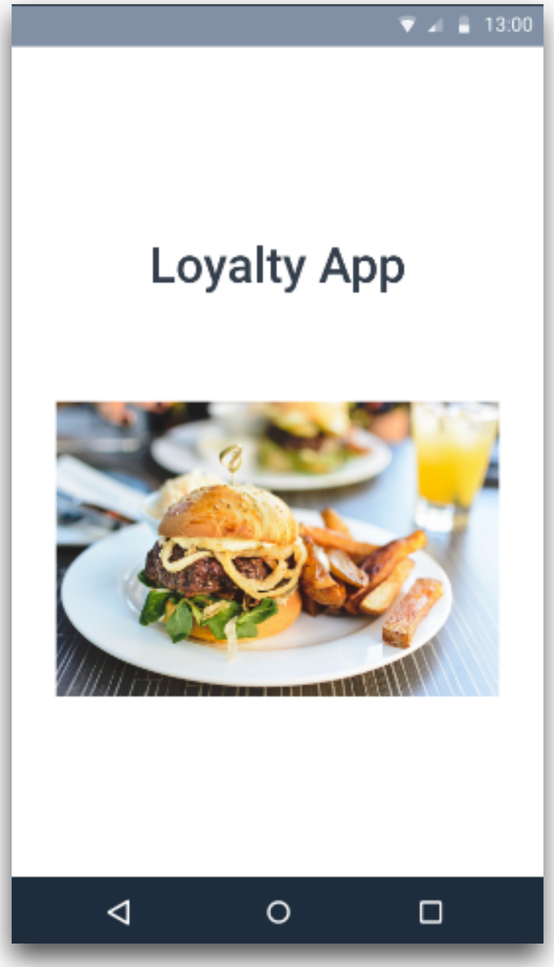

Once upon
a time...

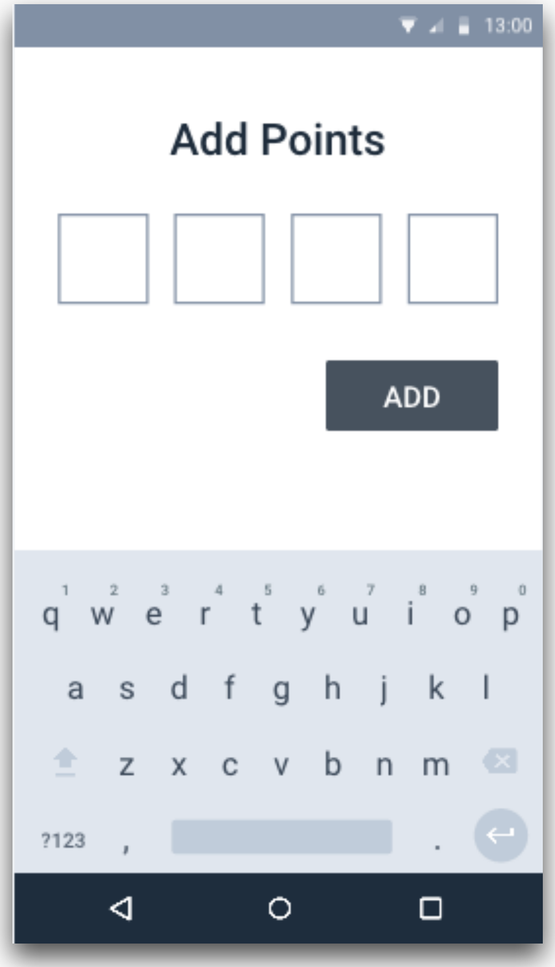
Once upon a time...

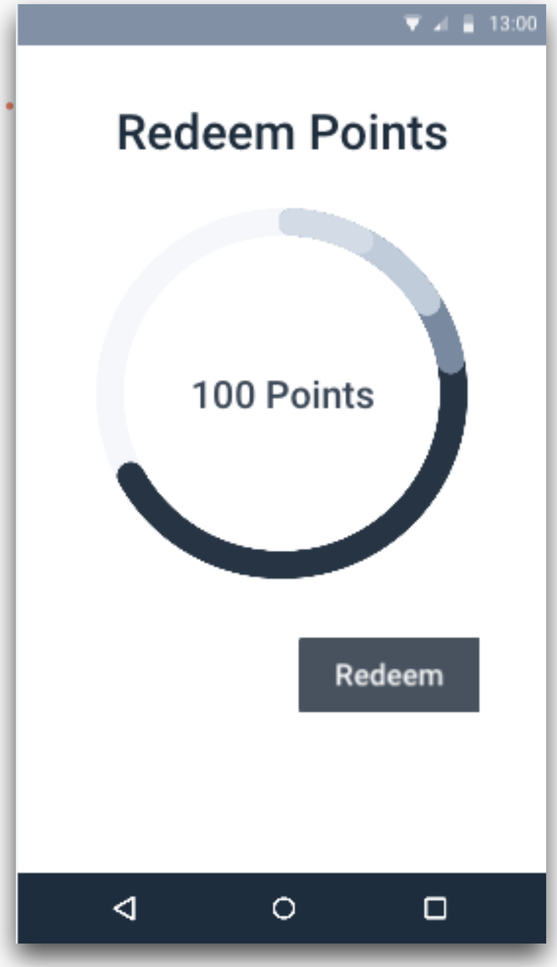


ORACLE Developer Champion

Free Hamburgers







What could go wrong?

ORACLE
Developer
Champion

What could go wrong?

- **Layalty Programs** are a Marketing Strategy
- **Don’t** represent a loss for the company

BUT

- They started to **lose money** for the Loyalty Program

What could go wrong?

- **Layalty Programs** are a Marketing Strategy
- **Don’t** represent a loss for the company

BUT

- They started to **lose money** for the Loyalty Program

What was wrong?

ORACLE
Developer
Champion

What was wrong?

GET
http://AmazingHamburguers.com/addPoints?user=qwer&code=7834

GET
http://AmazingHamburguers.com/register?
user=qwer&email=demo@gmail.com&password=q1w2e3r4t5y6

GET
http://AmazingHamburguers.com/login?
user=qwer&password=q1w2e3r4t5y6

What was wrong?

Exposed Params

GET
http://AmazingHamburguers.com/addPoints?user=qwer&**code=7834**

HTTP Method

GET
http://AmazingHamburguers.com/register?
user=qwer&email=demo@gmail.com&password=q1w2e3r4t5y6

SSL/TLS Absence

GET
http://AmazingHamburguers.com/login?
user=qwer&password=q1w2e3r4t5y6

ORACLE
Developer
Champion

What was wrong?

- Emails, Password and **Codes** were exposed
- A company lost money
- Someone lost his job

How to solve this issue?

ORACLE
Developer
Champion

How to solve this issue?

- Use an information exchange protocol, like JSON
- Use a different HTTP Method than GET, like POST
- Use SSL/TLS certificate

How to solve this issue?

- POST https://AmazingHamburguers.com/addPoints?

```
{
  “user”:”qwer”,
  “code”:7834
}
```

How to solve this issue?

- POST https://AmazingHamburguers.com/addPoints?

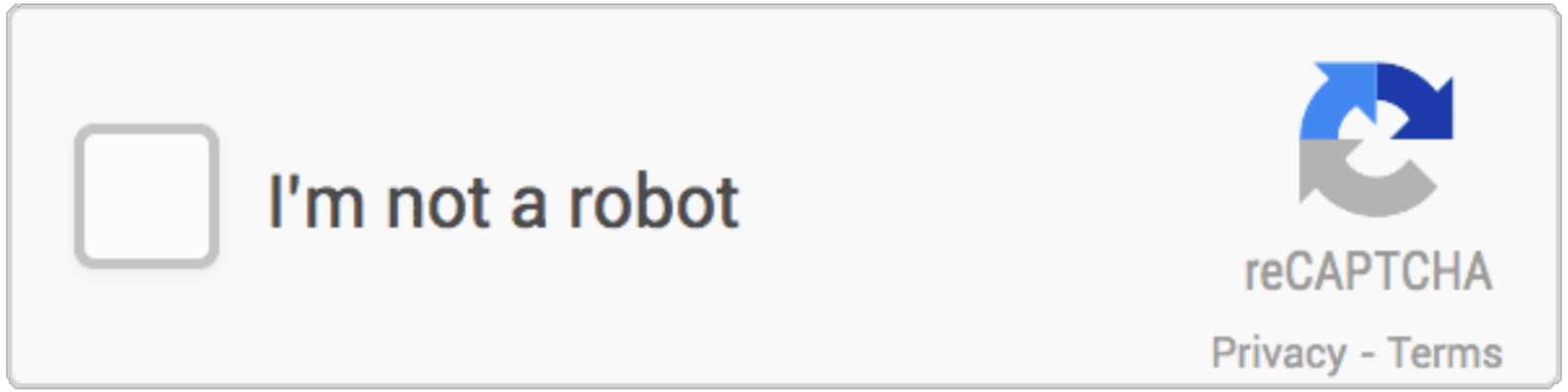
```
{
  “user”:”qwer”,
  “code”:7834
}
```

With SSL/TLS
Will travel encrypted

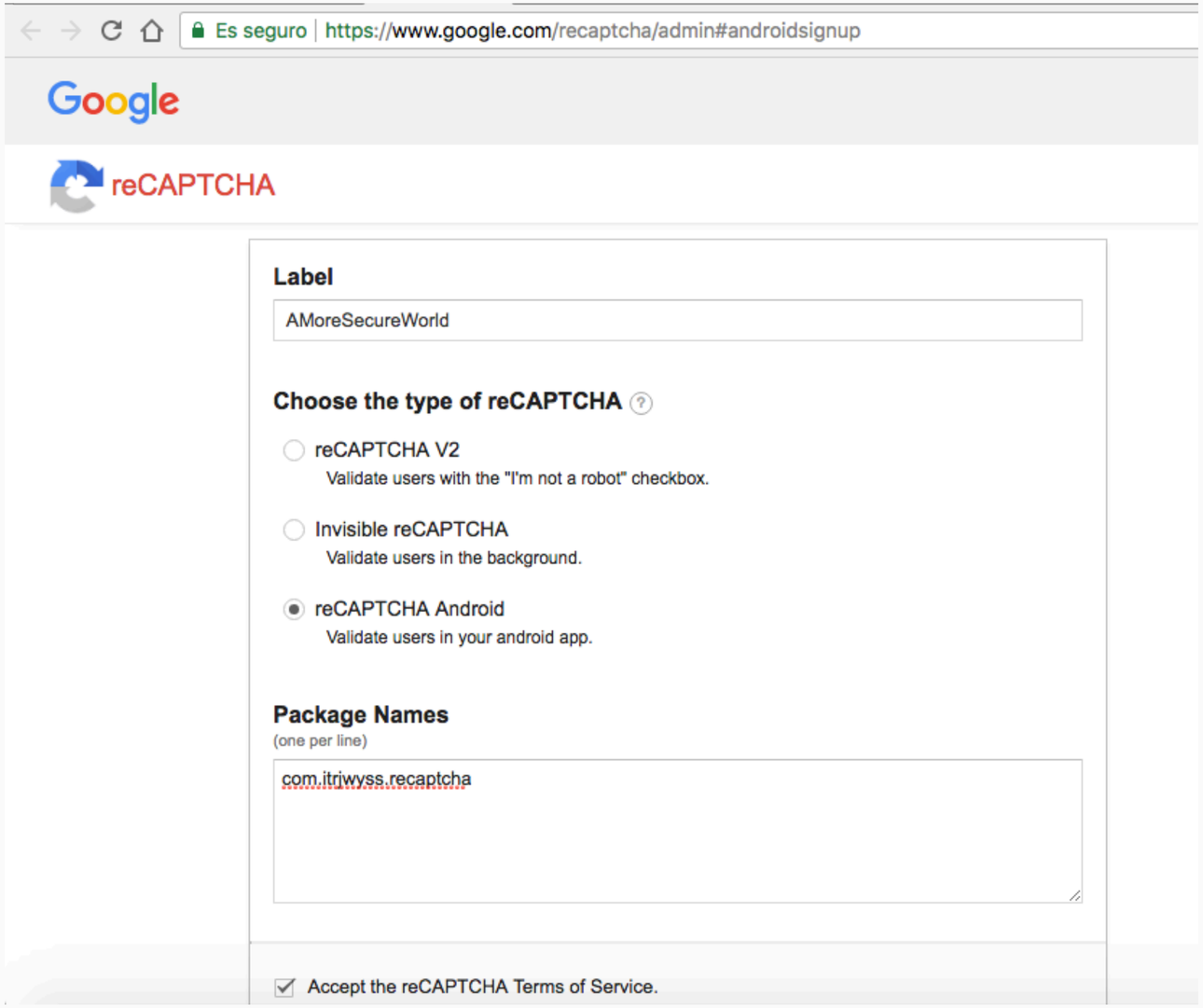
Human Verification

ORACLE Developer Champion

reCAPTCHA

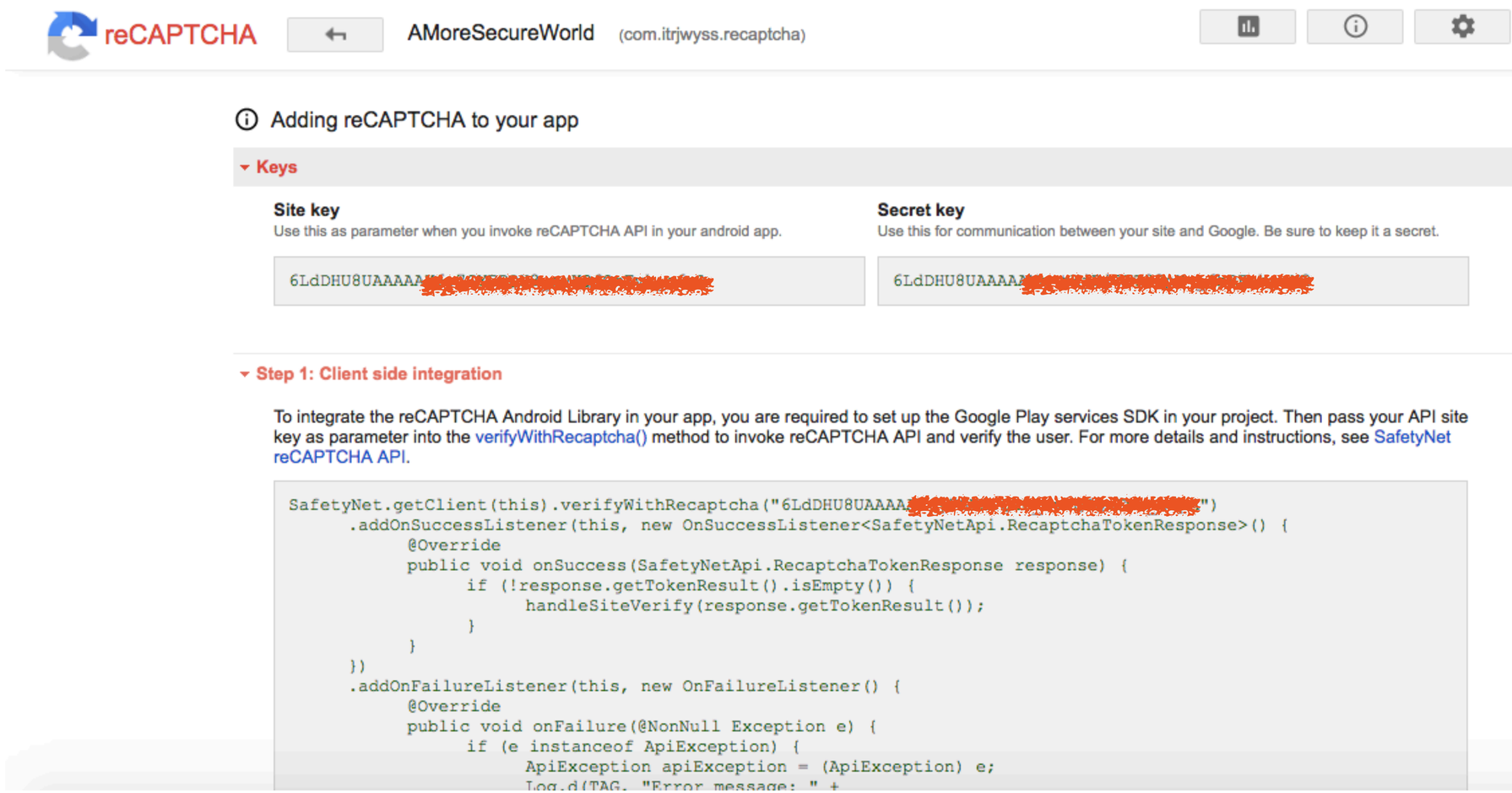


Create the Site



ORACLE Developer Champion

Create the Site



Adding Dependency

```
dependencies {
    //reCAPTCHA
    compile 'com.google.android.gms:play-services-safetynet:12.0.0'
}
```

ORACLE Developer Champion

reCAPTCHA

```
SafetyNet.getClient(this).verifyWithRecaptcha("6LdDHU8UAA[redacted]")
        .addOnSuccessListener(this) { response ->
            if (!response.tokenResult.isEmpty()) {
                Log.d(TAG, "TokenResult: " + response.tokenResult)
            }
        }
        .addOnFailureListener(this) { e ->
            if (e is ApiException) {
                Log.d(TAG, "Error message: " + CommonStatusCodes.getStatusCodeString(e.statusCode))
            } else {
                Log.d(TAG, "Unknown type of error: " + e.message)
            }
        }
```

reCAPTCHA

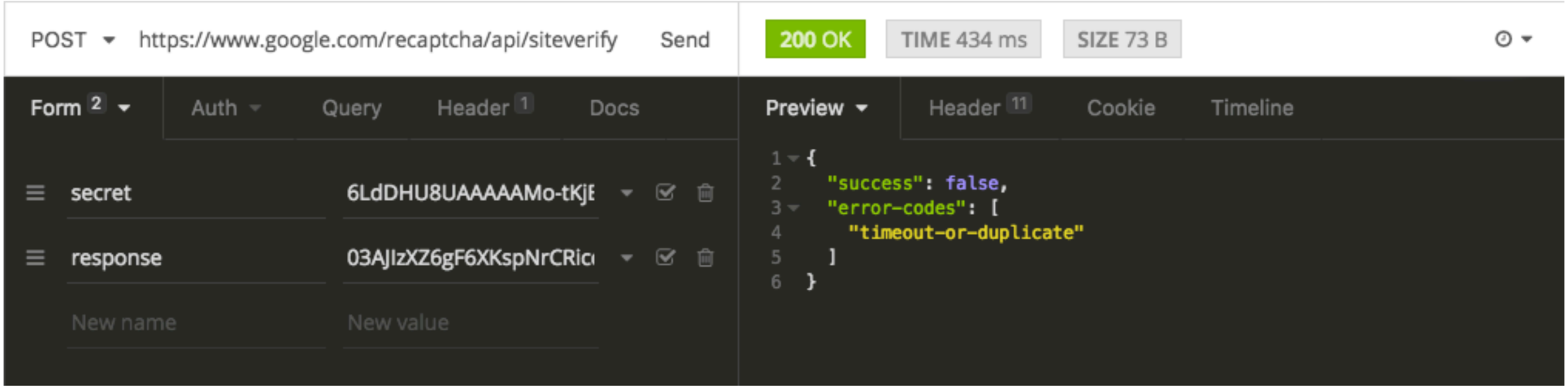
```
SafetyNet.getClient(this).verifyWithRecaptcha("6LdDHU8UAA[redacted]")
        .addOnSuccessListener(this) { response ->
            if (!response.tokenResult.isEmpty()) {
                Log.d(TAG, "TokenResult: " + response.tokenResult)
            }
        }
        .addOnFailureListener(this) { e ->
            if (e is ApiException) {
                Log.d(TAG, "Error message: " + CommonStatusCodes.getStatusCodeString(e.statusCode))
            } else {
                Log.d(TAG, "Unknown type of error: " + e.message)
            }
        }
```

Verify the result

reCAPTCHA

ORACLE Developer Champion

reCAPTCHA


POST
https://www.google.com/recaptcha/api/siteverify
Send
200 OK
TIME 434 ms
SIZE 73 B
Form 2
Auth
Query
Header 1
Docs
Preview
Header 11
Cookie
Timeline
secret
6LdDHU8UAAAAAMo-tKjE
response
03AJIzXZ6gF6XKspNrCRic
New name
New value
1 {
2 "success": false,
3 "error-codes": [
4 "timeout-or-duplicate"
5]
6 }


AMBASSADOR

reCAPTCHA

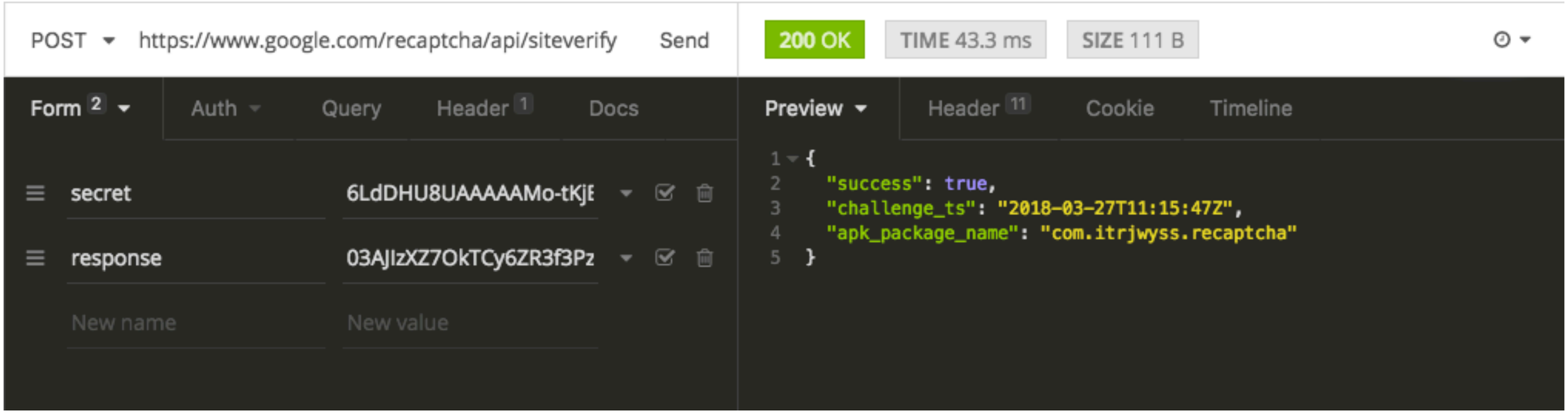
```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.itrjwyss.recaptcha">

    <uses-permission android:name="android.permission.INTERNET" />

    <application
```

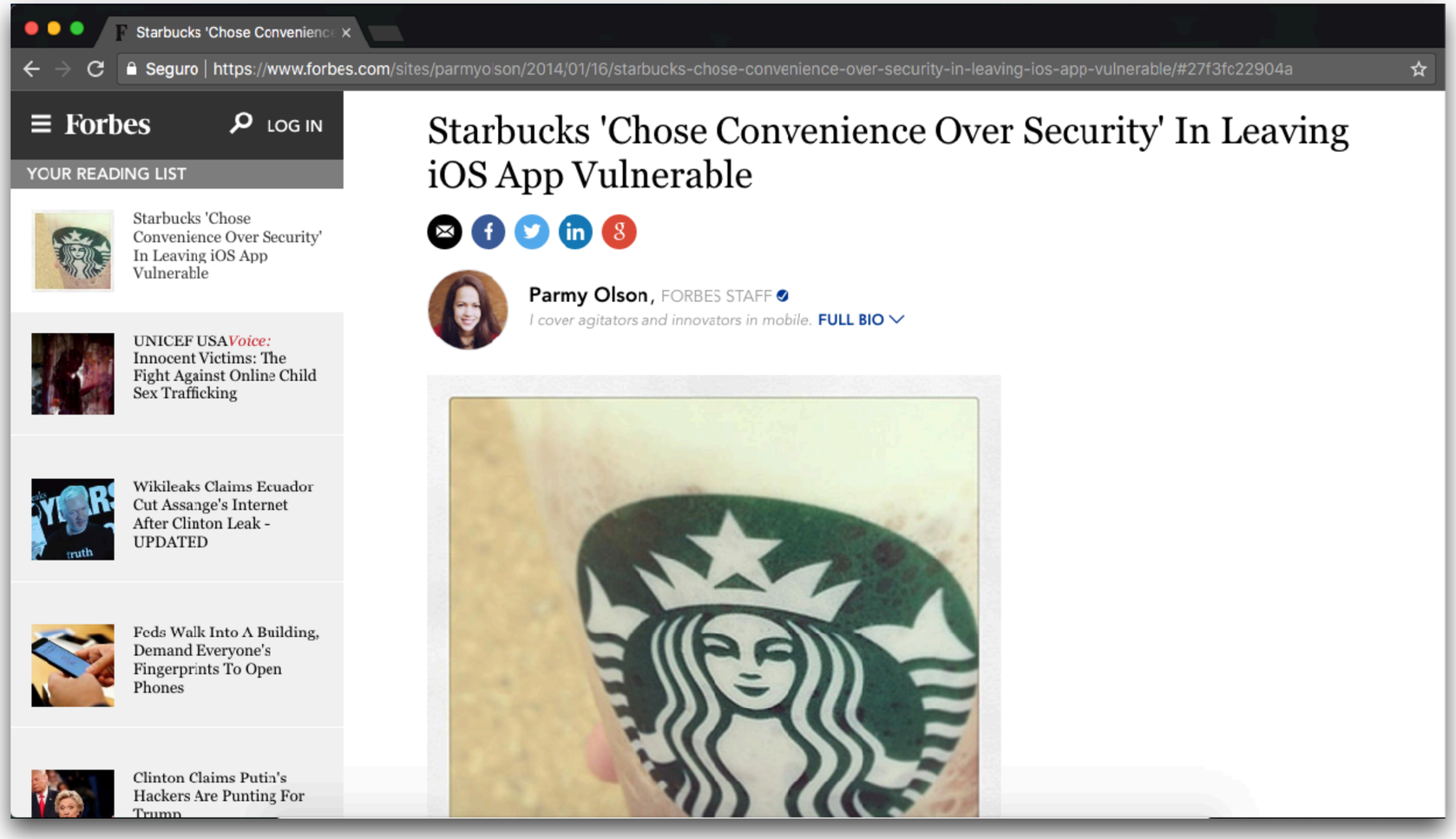
ORACLE
Developer
Champion

reCAPTCHA



AMBASSADOR

“Convenience Over Security”



ORACLE Developer Champion

What was wrong?

- Was storing data about users in plain text and locally on a device (public access)
- Emails, Passwords and geolocation data

What was wrong?

Public Access

- Was storing data about users in plain text and locally on a device (public access)

Unencrypted Data

- Emails, Passwords and geolocation data

How to solve this issue?

ORACLE
Developer
Champion

How to solve this issue?

- Save the information so that only our application has access to it.
    - SharedPreferences
    - Storage (Internal)

Shared Preferences

```
SharedPreferences sharedPref = context.getSharedPreferences(
        getString(R.string.preference_file_key), Context.MODE_PRIVATE);
```

```
SharedPreferences.Editor editor = sharedPref.edit();
editor.putString(getString(R.string.id), id);
editor.commit();
```

```
sharedPref.getString(getString(R.string.id), defaultValue);
```

Shared Preferences

```
SharedPreferences sharedPref = context.getSharedPreferences(
        getString(R.string.preference_file_key), Context.MODE_PRIVATE);
```

Restrict Access only to my App

```
SharedPreferences.Editor editor = sharedPref.edit();
editor.putString(getString(R.string.id), id);
editor.commit();
```

```
sharedPref.getString(getString(R.string.id), defaultValue);
```

ORACLE Developer Champion

Internal Storage

- By default those files are accessible only to your app.

```
File file = new File(context.getFilesDir(), filename);
```

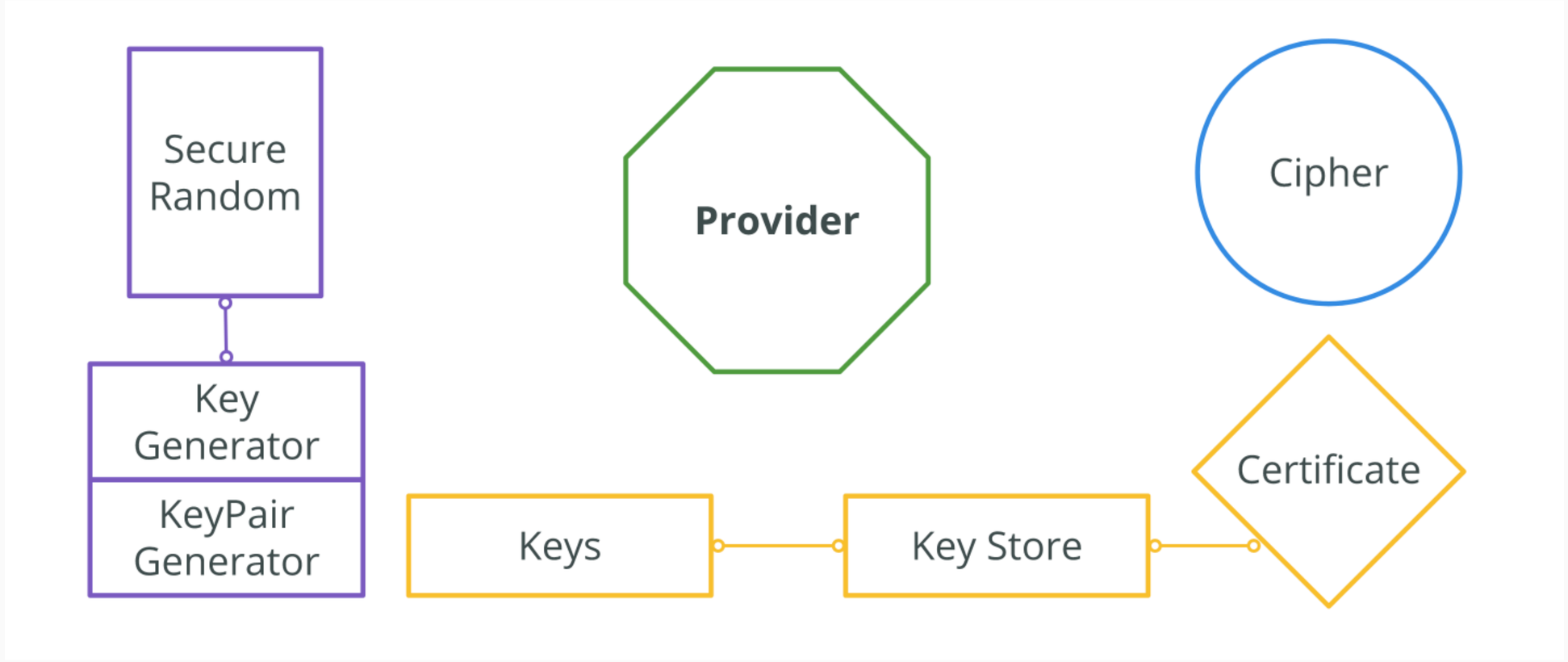
Internal Storage

```
String filename = "myfile";
String string = “The email, The password”;
FileOutputStream outputStream;

try {
  outputStream = context.openFileOutput(filename, Context.MODE_PRIVATE);
  outputStream.write(string.getBytes());
  outputStream.close();
} catch (Exception e) {
  e.printStackTrace();
}
```

We can encrypt the information

Java Cryptography Architecture



ORACLE Developer Champion

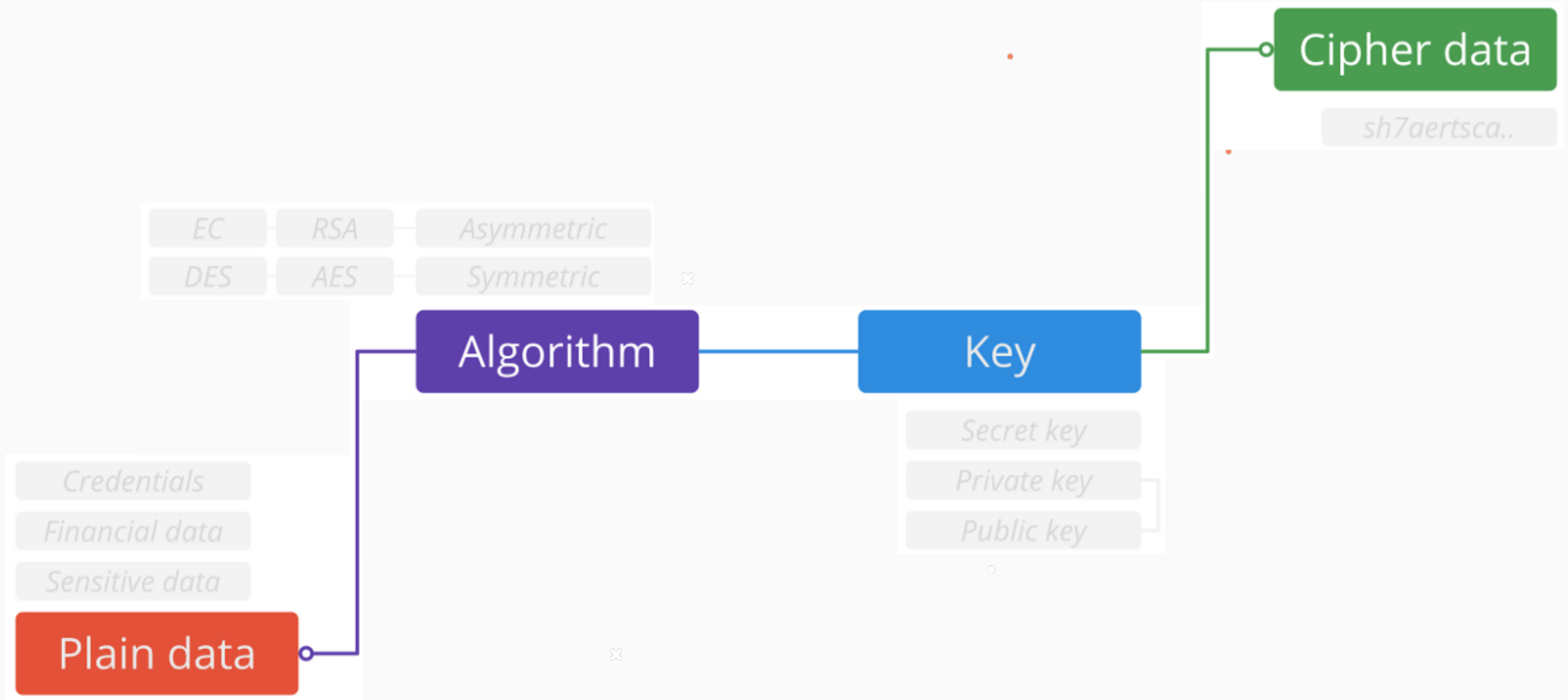
AndroidKeyStore

- Java Cryptography Implementaion
    - Key material may be bound to the secure hardware (Trust Zone)
    - Asymmetric keys from 18+
    - Symmetric keys from 23+

Cipher

Algorithm	Supported (API Levels)
AES/CBC/NoPadding	23+
AES/CBC/PKCS7Padding	23+
AES/CTR/NoPadding	23+
AES/ECB/NoPadding	23+
AES/ECB/PKCS7Padding	23+
AES/GCM/NoPadding	23+
RSA/ECB/NoPadding	18+
RSA/ECB/PKCS1Padding	18+
RSA/ECB/OAEPWithSHA-1AndMGF1Padding	23+
RSA/ECB/OAEPWithSHA-224AndMGF1Padding	23+
RSA/ECB/OAEPWithSHA-256AndMGF1Padding	23+
RSA/ECB/OAEPWithSHA-384AndMGF1Padding	23+
RSA/ECB/OAEPWithSHA-512AndMGF1Padding	23+
RSA/ECB/OAEPPadding	23+

Cryptography Process



Cipher

```
fun encrypt(data: String, key: Key?): String {
    cipher.init(Cipher.ENCRYPT_MODE, key)
    val bytes = cipher.doFinal(data.toByteArray())
    return Base64.encodeToString(bytes, Base64.DEFAULT)
}
```

Cipher

```
fun decrypt(data: String, key: Key?): String {
    cipher.init(Cipher.DECRYPT_MODE, key)
    val encryptedData = Base64.decode(data, Base64.DEFAULT)
    val decodedData = cipher.doFinal(encryptedData)
    return String(decodedData)
}
```

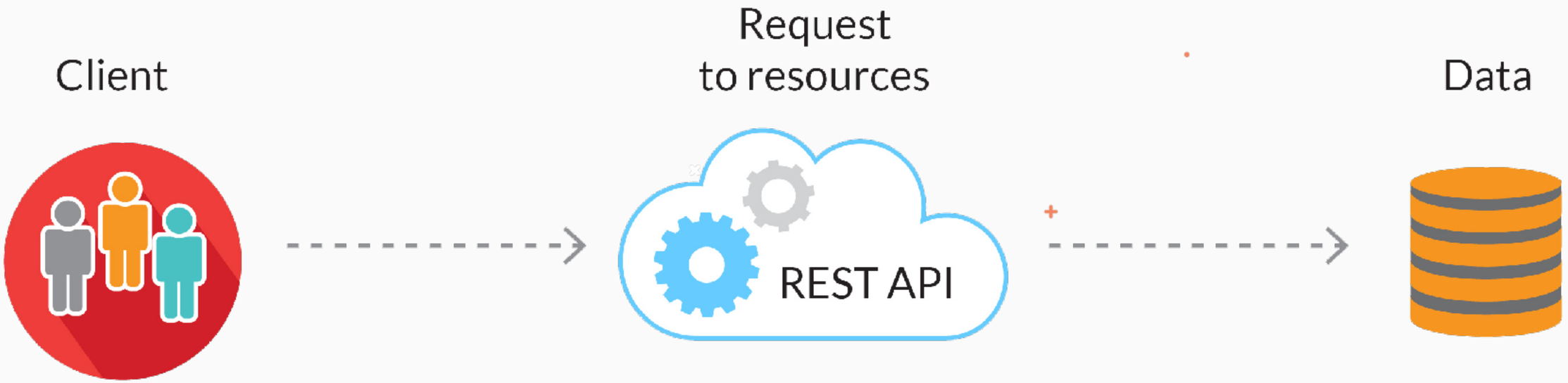
Security Myth

ORACLE
Developer
Champion

Security Myth

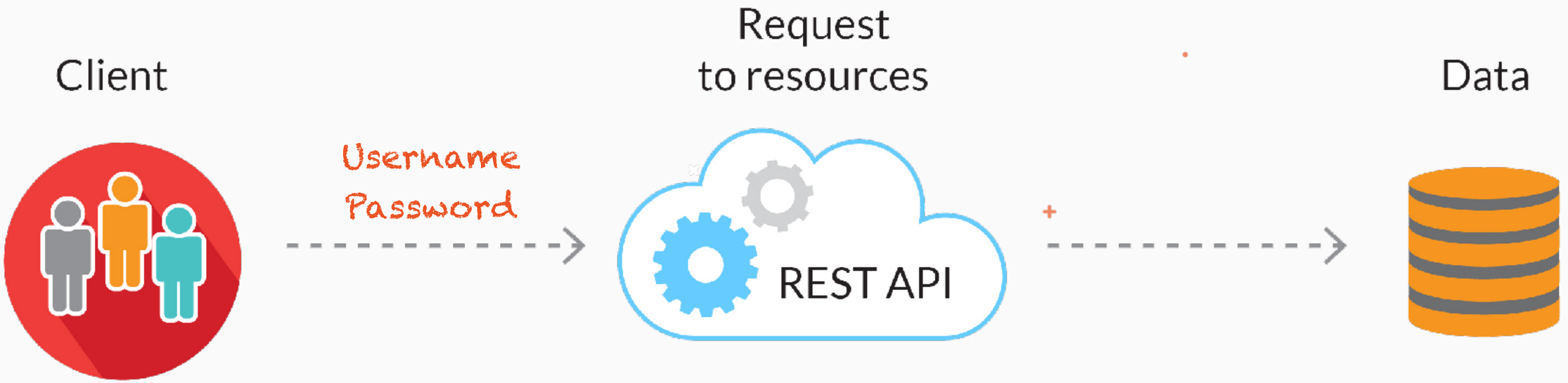
- **“Is it better for mobile apps to be easy-to-use, or secure?”**
- User Friendly vs Security
- Permanent open session
- OAuth (2006, 2010)

Bad API Design



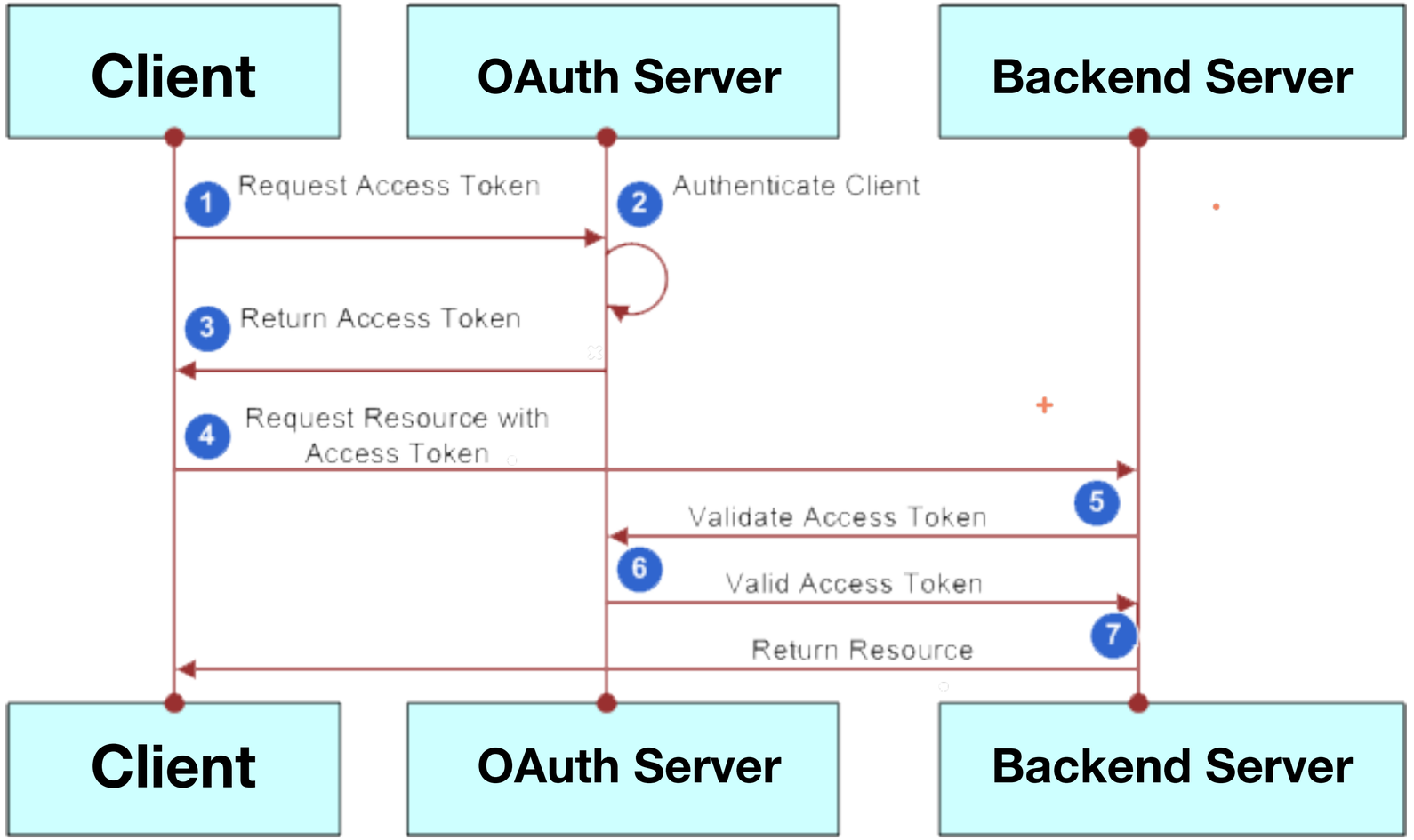
ORACLE Developer Champion

Bad API Design



ORACLE Developer Champion

OAuth


Client
OAuth Server
Backend Server
1
Request Access Token
2
Authenticate Client
3
Return Access Token
4
Request Resource with Access Token
5
Validate Access Token
6
Valid Access Token
7
Return Resource
Client
OAuth Server
Backend Server


AMBASSADOR

ORACLE
Developer
Champion

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.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

Claims

JSON Web Signature
JWT + JWS

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
```


How Works the Signature?

```
{
  "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
)
```

ORACLE
Developer
Champion

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

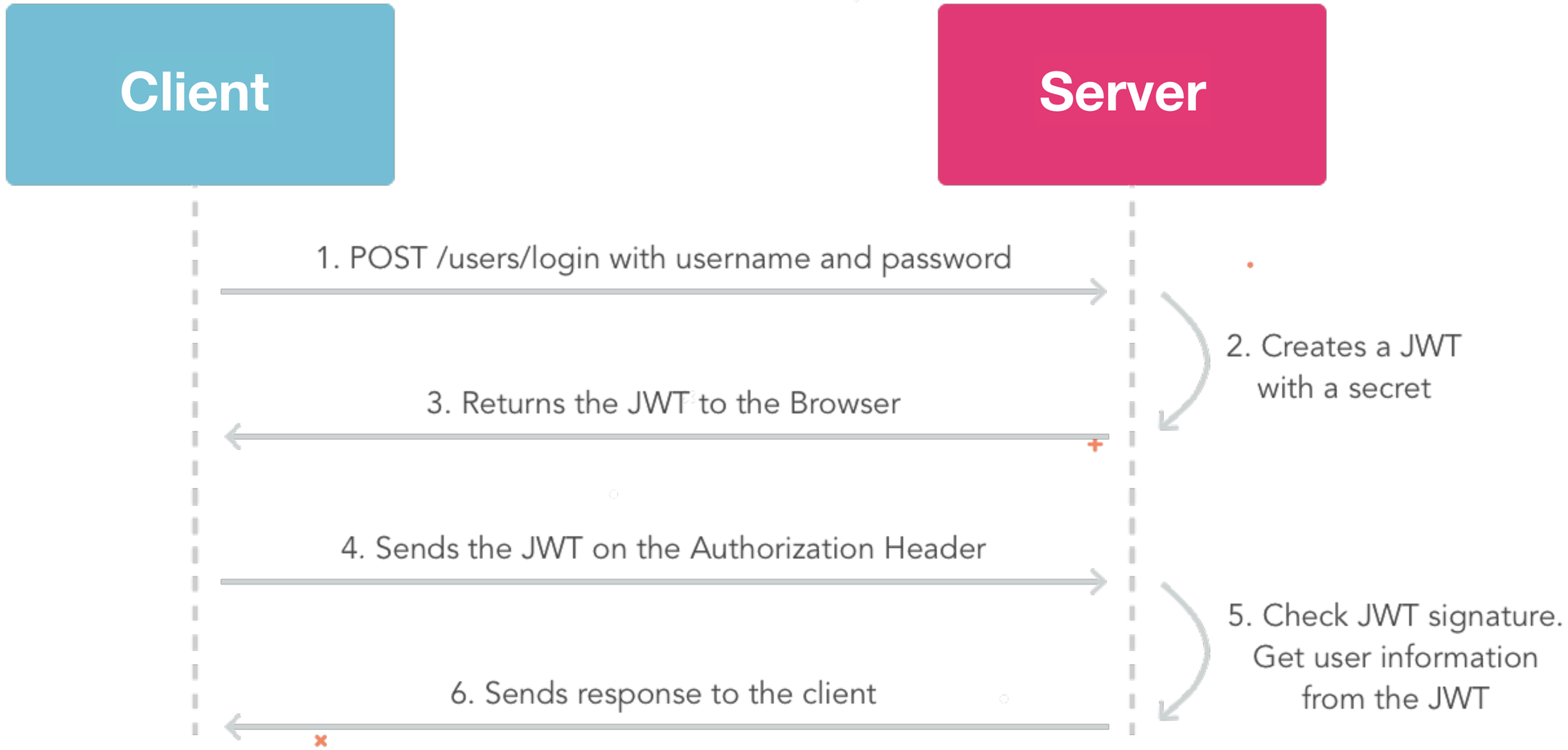
iss	The issuer of the token
sub	The subject of the token
aud	The audience of the token
exp	The expiration in NumericDate value
nbf	sbt configuration files
iat	The time the JWT was issued
jti	Unique identifier for the JWT

What problems does JWT solve?

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

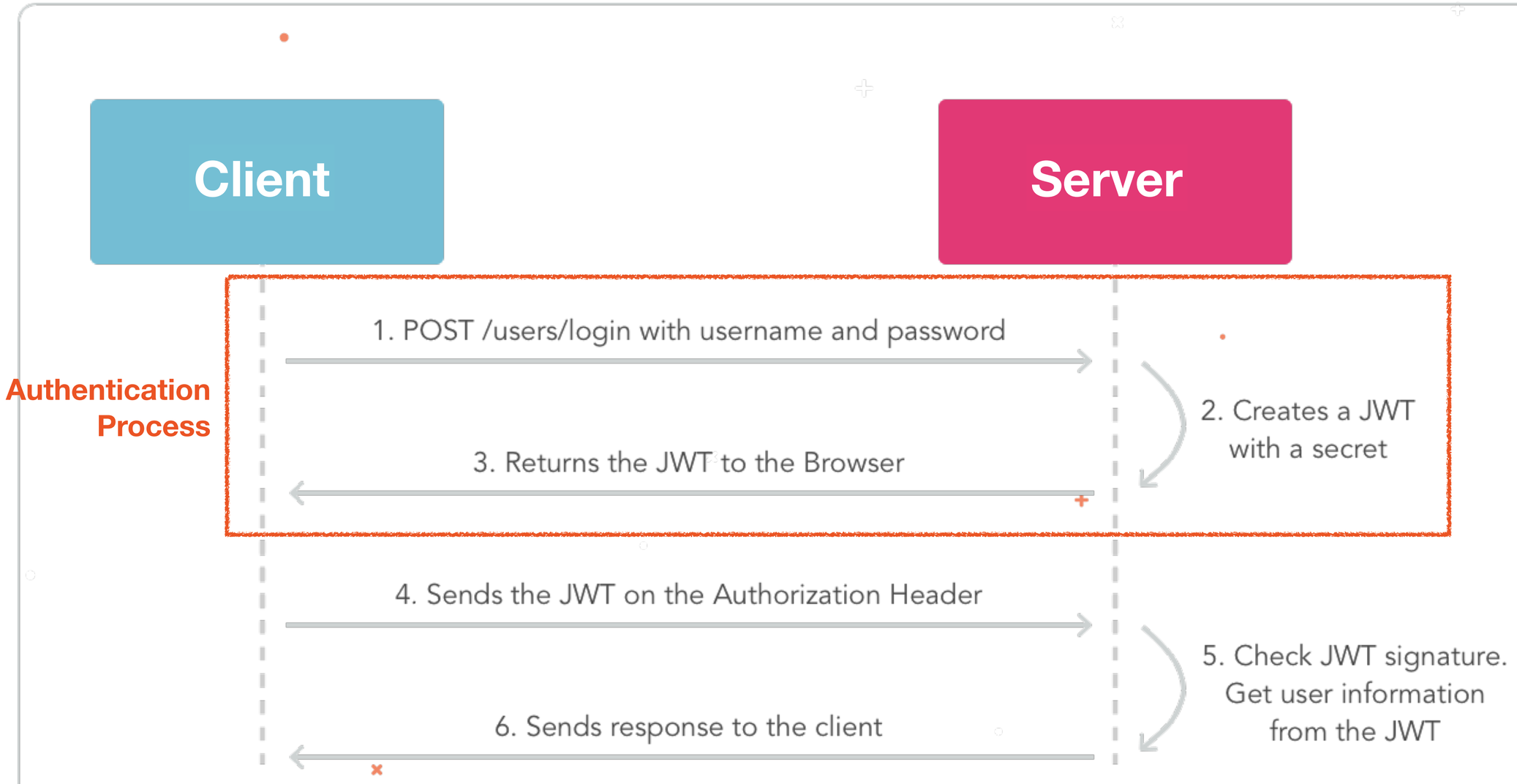
What problems does JWT solve?

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



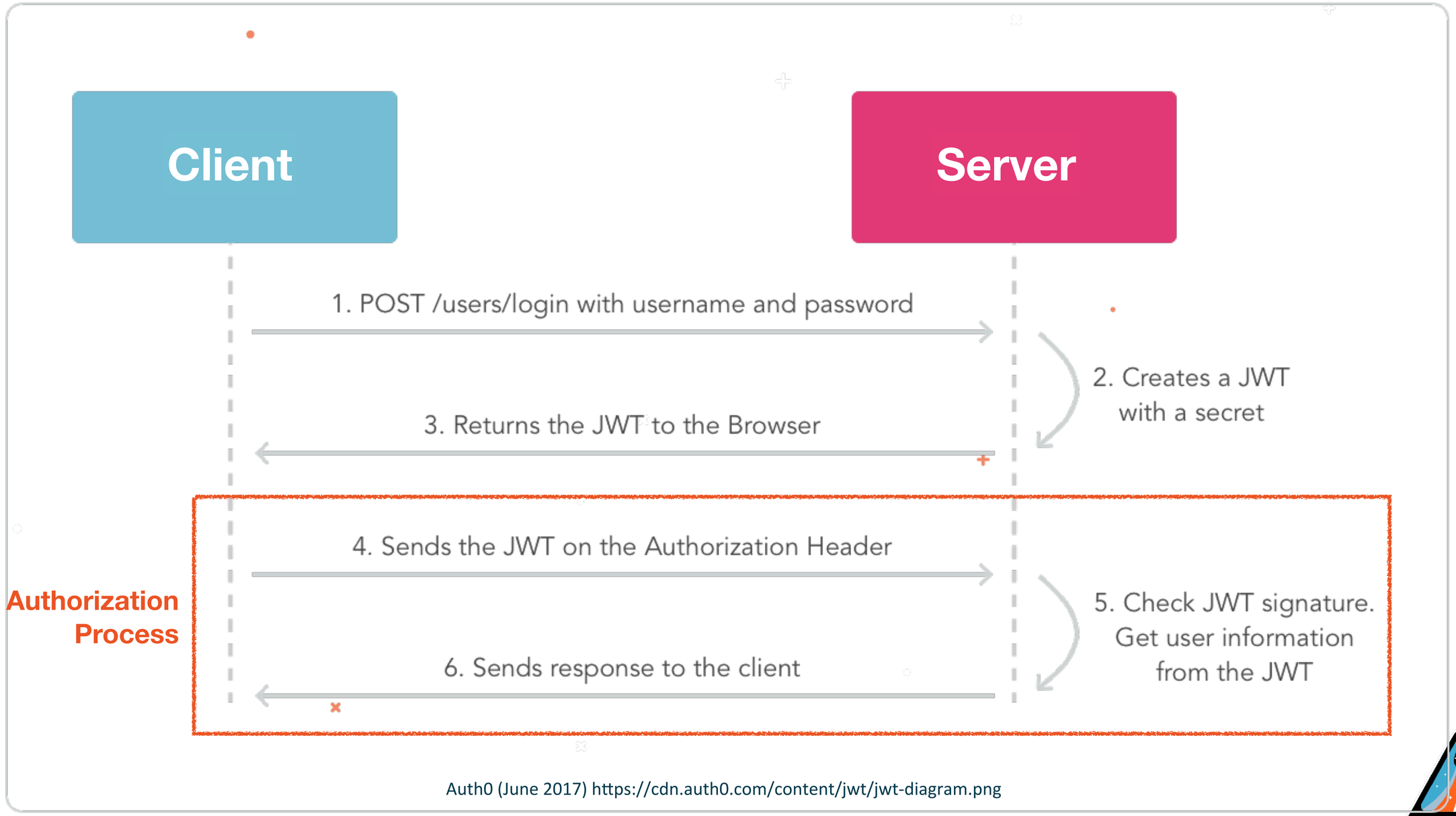
Auth0 (June 2017) https://cdn.auth0.com/content/jwt/jwt-diagram.png

AMBASSADOR



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

AMBASSADOR



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

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.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```


Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

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

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

auth0.com/e-books/jwt-handbook

AMBASSADOR

Fail Encryption

ORACLE Developer Champion

What happenned?

```
{
    "accountName":"Mercedes Wyss",
    “accountNumber":"1234567890"
}
```

What happenned?

```
{
    "accountName":"Mercedes Wyss",
    “accountNumber":"1234567890"
}
```

JjLYWa7gFBj7JVNogMTp37z24NQ74dYy6b8u5N8FO9NmyQeg
YVAuM17Duumvz9yLsHiz/RusnmelZgHol1QVKkl84pBt8bJm7/
e9qjY+dTc=

What happenned?

```
{
    "accountName":"Mercedes Wyss",
    “accountNumber":"1234567890"
}
```

```
{
    "accountName":"5cPRRpp/bUkcnNZ6CZ6efg==",
    “accountNumber":"yPGQm/a6y1My3IBHnpQEVA=="
}
```

What could go wrong?

ORACLE
Developer
Champion

What could go wrong?

```
{
    "accountName":"Mercedes Wyss",
    “accountNumber":"1234567890"
}
```

```
{
    "accountName":"5cPRRpp/bUkcnNZ6CZ6efg==",
    “accountNumber":"yPGQm/a6y1My3IBHnpQEVA=="
}
```

What could go wrong?

```
{
    "accountName":"Mercedes Wyss",
    “accountNumber":"1234567890"
}
```

Unencrypted and Encripted values

```
{
    "accountName":"5cPRRpp/bUkcnNZ6CZ6efg==",
    “accountNumber":"yPGQm/a6y1My3IBHnpQEVA=="
}
```

Reverse Engineering

ORACLE
Developer
Champion

Reverse Engineering

```
{
    "accountName":"Mercedes Wyss",
    “accountNumber":"1234567890"
}
```

Unencrypted and Encripted values

```
{
    "accountName":"5cPRRpp/bUkcnNZ6CZ6efg==",
    “accountNumber":"yPGQm/a6y1My3IBHnpQEVA=="
}
```

What went wrong?

- If I **have** the encrypted and unencrypted values, I can **found** the Secret Key and Encryption Algorithm

JSON Web Encryption
JWE

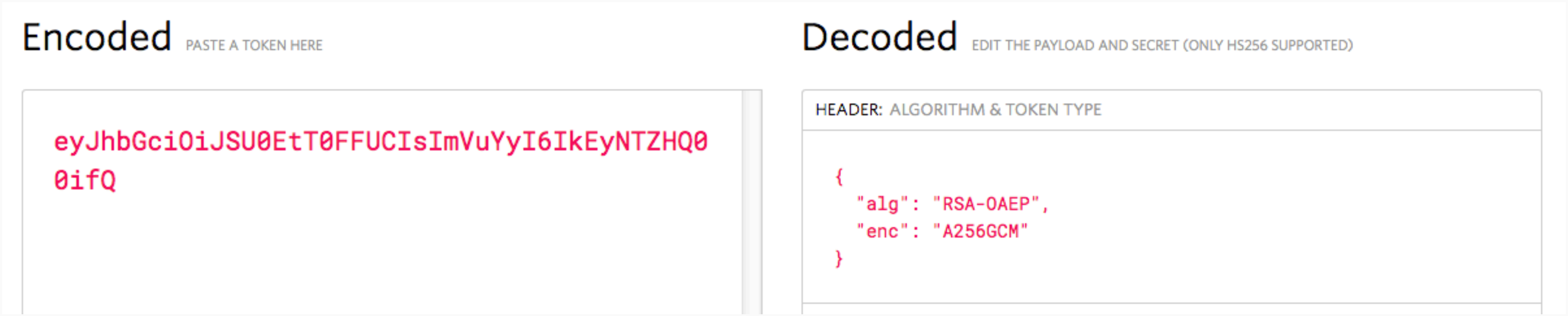
JSON Web Encryption

- The JWE Protected Header
- The JWE Encrypted Key
- The JWE Initialization Vector
- The JWE Ciphertext
- The JWE Authentication Tag

ORACLE
Developer
Champion

eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00ifQ.
OKOawDo13gRp2ojaHV7LFpZcgV7T6DVZKTyKOMTYUmKoTCVJRgckCL
9kiMT03JGeipsEdY3mx_etLbbWSrFr05kLzcSr4qKAq7YN7e9jwQRb
23nfa6c9d-
StnImGyFDbSv04uVuxIp5Zms1gNxKKK2Da14B8S4rzVRltdYwam_lD
p5XnZAYpQdb76FdIKLaVmqgfwX7XWRxv2322i-
vDxRfqNzo_tETKzpVLzfiwQyeyPGLBIO56YJ7eObdv0je81860ppam
avo35UgoRdbYaBcoh9QcfylQr66oc6vFWXRcZ_ZT2LawVCWTIy3brG
Pi6UklfCpIMfIjf7iGdXKHzg.
48V1_ALb6US04U3b.
5eym8TW_c8SuK0ltJ3rpYIzOeDQz7TALvtu6UG9oMo4vpzs9tX_EFS
hS8iB7j6jiSdiwkIr3ajwQzaBtQD_A.
XFBoMYUZodetZdvTiFvSkQ

- This JWE employs RSA-OAEP for key encryption and A256GCM for content encryption



ORACLE Developer Champion

JWE Protected Header

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJFQ0RILUVTK0ExMjhLVyIsImVuYyI6Ik
ExMjhDQkMtSFMyNTYiLCJlcGsiOnsia3R5IjoiRUMi
LCJ4IjoiWE9YR1E5XzZRQ3ZCZzN1OHZDSS1VZEJ2SU
NBRWNOTkJyZnFkN3RHN29RNCIsInkiOiJoUW9XTm90
bk56S2x3aUNuZUprTElxRG5UTnc3SXNkQkM1M1ZVcV
ZqVkpjIiwiY3J2IjoiUC0yNTYifX0
```


Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "alg": "ECDH-ES+A128KW",
  "enc": "A128CBC-HS256",
  "epk": {
    "kty": "EC",
    "x": "XOXGQ9_6QCvBg3u8vCI-UdBvICAEcNNBrfqd7tG7oQ4",
    "y": "hQoWNotnNzKlwiCneJkLIqDnTNw7IsdBC53VUqVjVJc",
    "crv": "P-256"
  }
}
```


AMBASSADOR

Identity Management

ORACLE Developer Champion

Firebase

Authentication

AMBASSADOR

Firebase Auth

- Anonymous Authentication
- Management (name, email, photoURL, password)
- Multiple Auth Providers (Federated Identity)
- Passwordless (email link, phone number)

ORACLE
Developer
Champion


Auth0
The new way to solve Identity
var lock = new Auth0Lo
connections: [
en
#333814
closable: false
icon: http://au
gravatar: false
lock.show();
FB
1:20 PM
77%
Welcome Peter
peter@auth0.com
Don't remember your password?
LOG IN

Modern Identity Platform

The enterprise-grade platform for modern identity.

Single Sign On

Connect WordPress to every login system on Earth. Really.

Lock

The Auth0 Login Box. Secure your websites and mobile apps.

Breached Passwords Detection

Protect your users and services from password leaks.

User Management

The simplest and easiest to use tools to help administrators manage users.

Multifactor Authentication

The most usable and friction-free multifactor authentication experience.

Passwordless

Allow users to login without the need to remember a password.

Auth0

- Management (I can define the info)
- Define roles
- More extensible Federated Identity, Passwordless
- Multifactor Authentication

Password Nightmare

ORACLE Developer Champion

Password Nightmare

The password must be contain

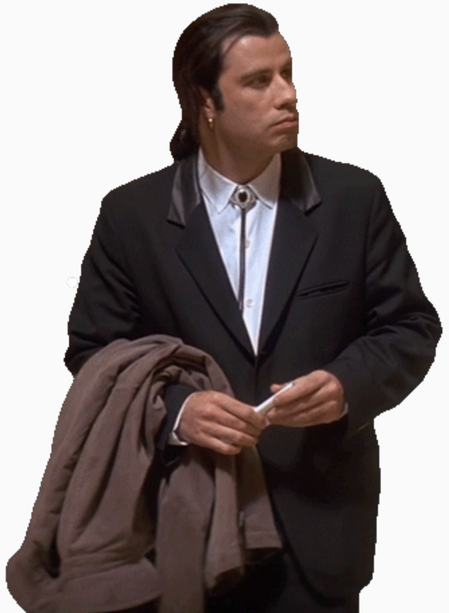
- At least one numerical character
- At least one uppercase character
- At least one lowercase character
- At least one symbol
- At least one hieroglyph
- The blood of a virgin
- The horn of a unicorn

Password Nightmare

- Wrong password!!!
- Wrong password!!!
- Me: Recovery and Change Password
- You need to use a different password than the previous one

Password Nightmare

- Wrong password!!!
- Wrong password!!!
- Me: Recovery and Change Password
- You need to use a different password than the previous one



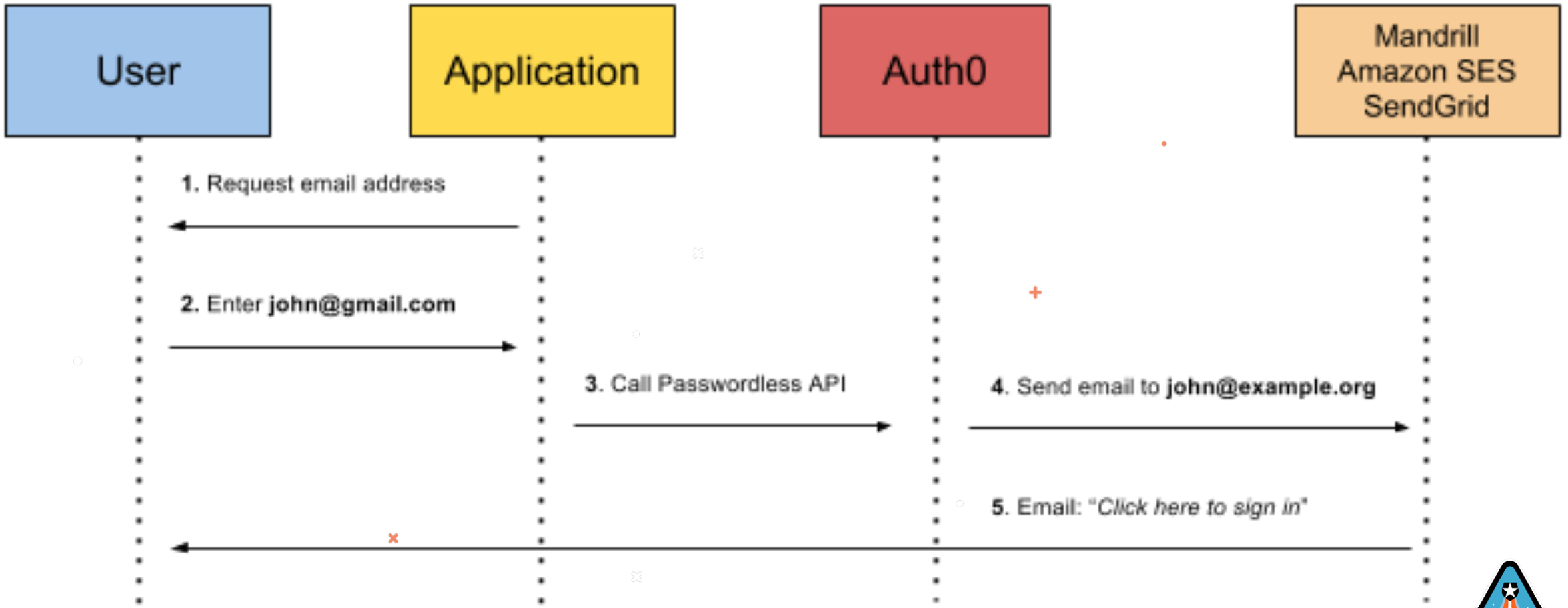
ORACLE Developer Champion

Passwordless & Federated Identity

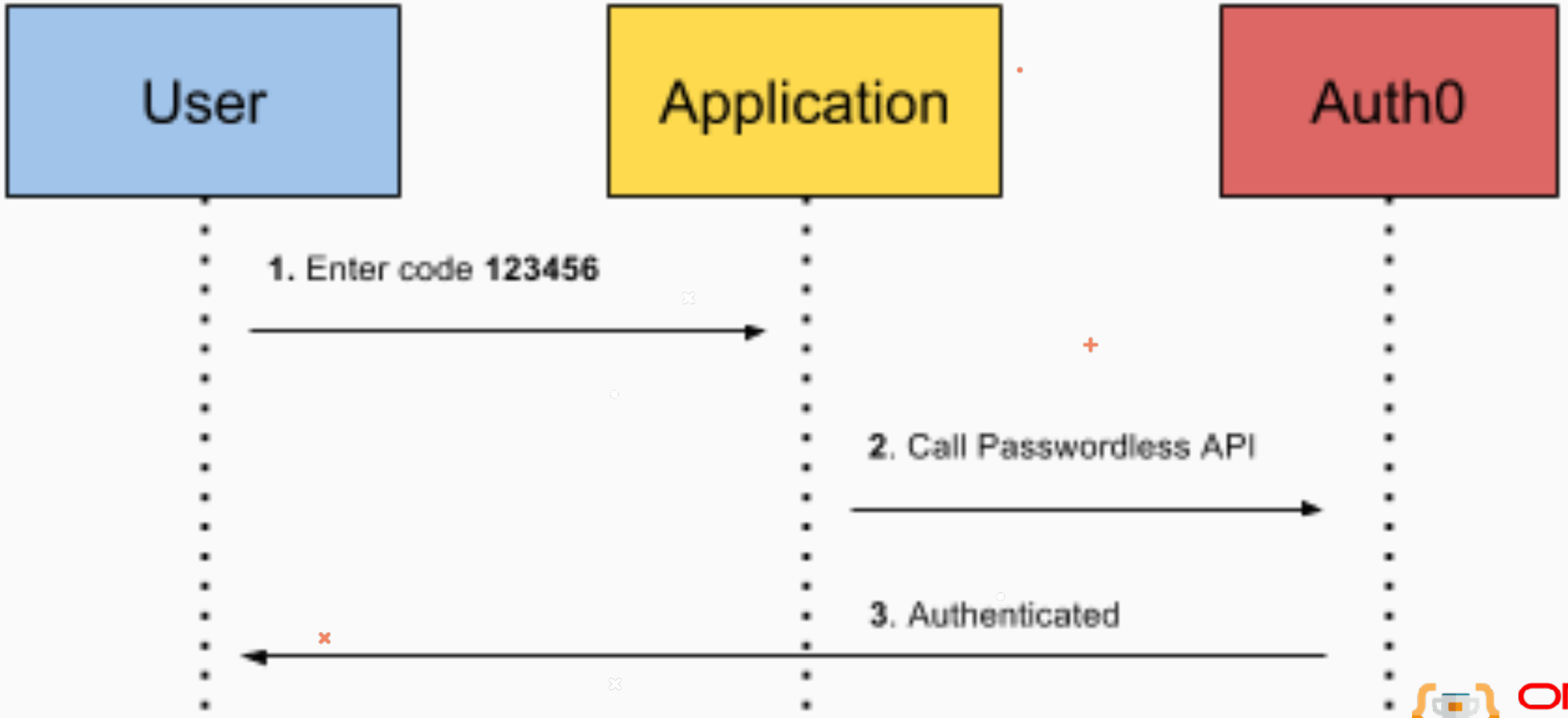
Passwordless

- Passwordless Authentication is a type of authentication where users do not need to login with passwords.
    - Authentication with a magic link via email
    - Authentication with a one-time code via email
    - Authentication with a one-time code via SMS
    - Authentication with Fingerprint

Passwordless by Email

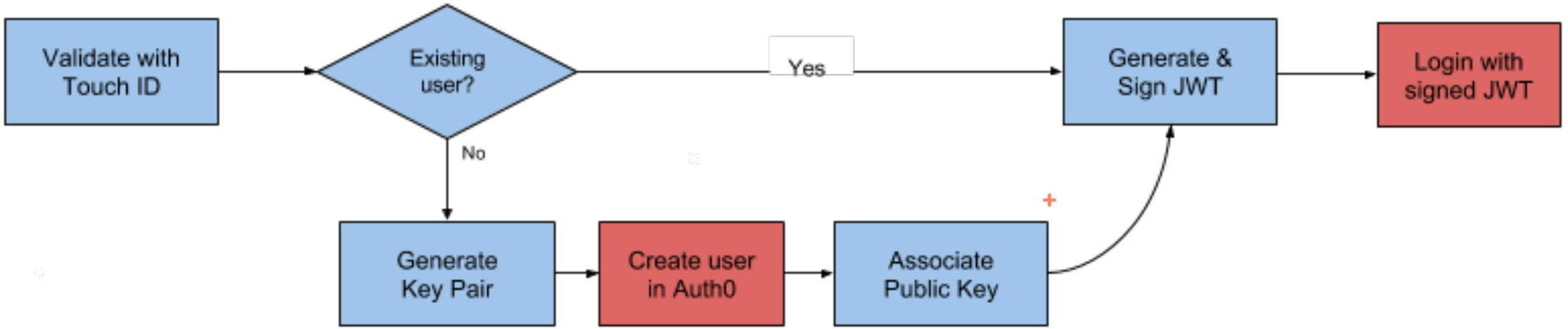


Passwordless by Code



ORACLE Developer Champion

Passwordless by Fingerprint



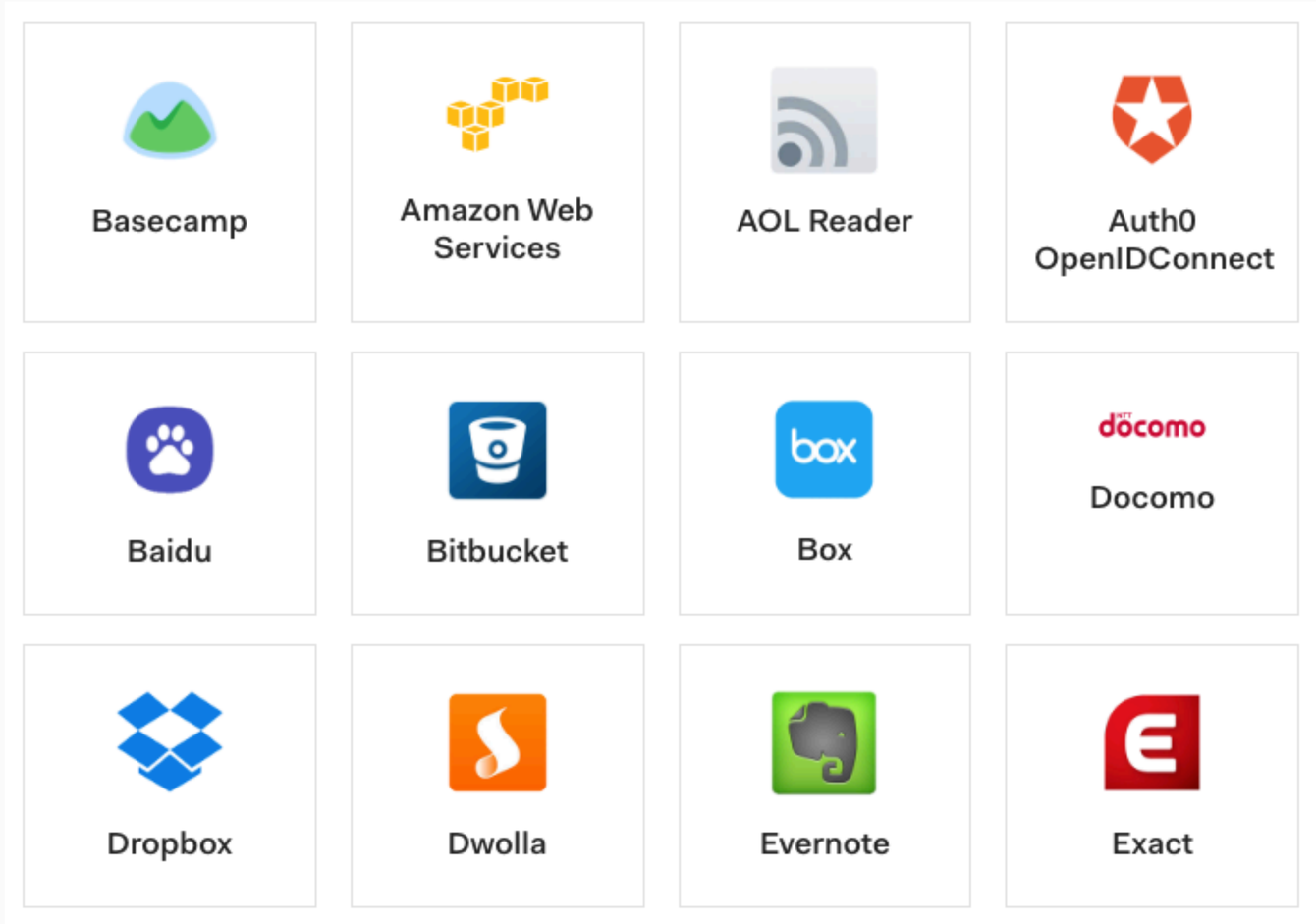
AMBASSADOR

Federated Identity

- Authenticate throw Federated Identities like Facebook, Twitter, Google.

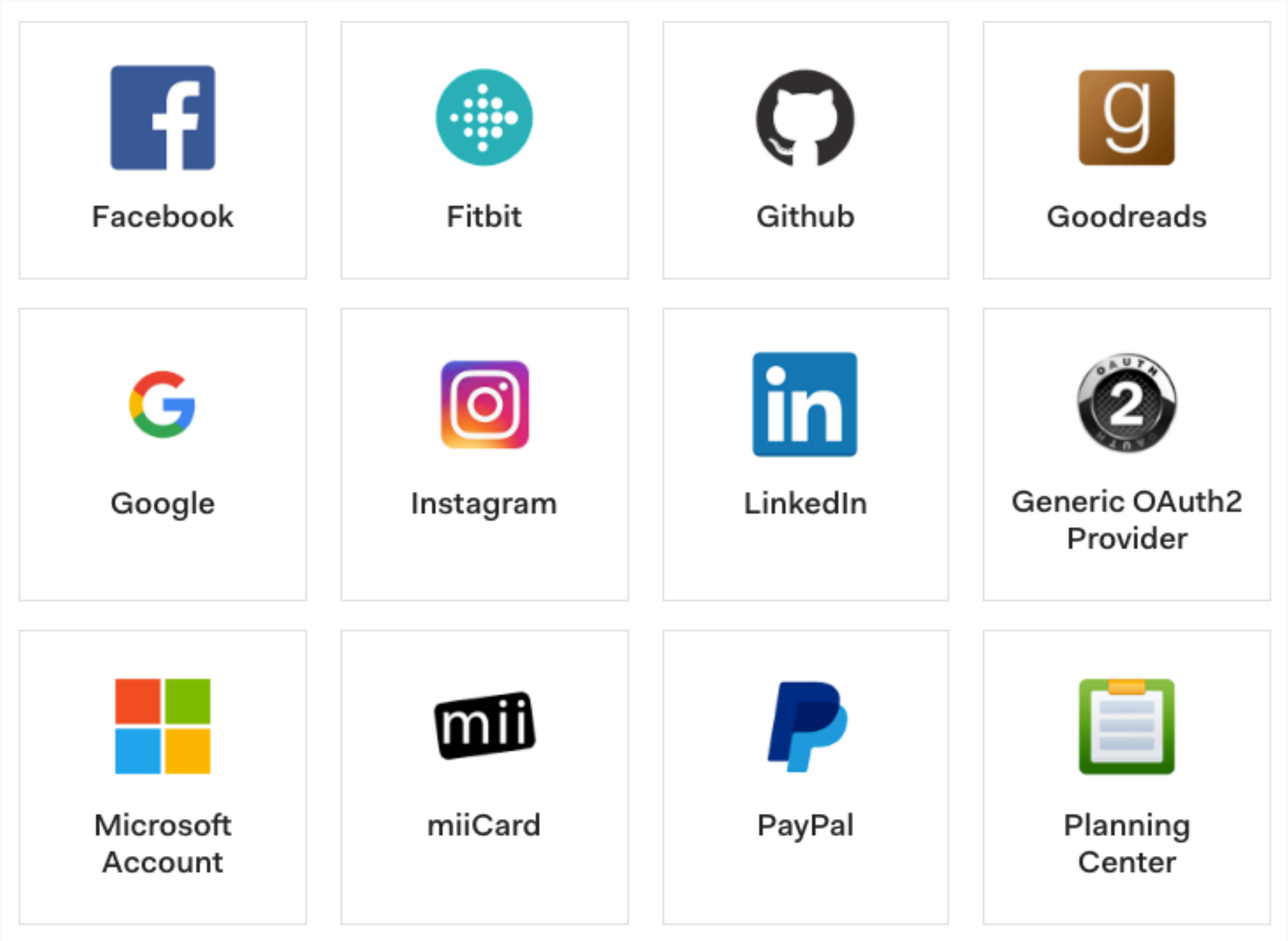
Federated Identity - Firebase

Federated Auth0



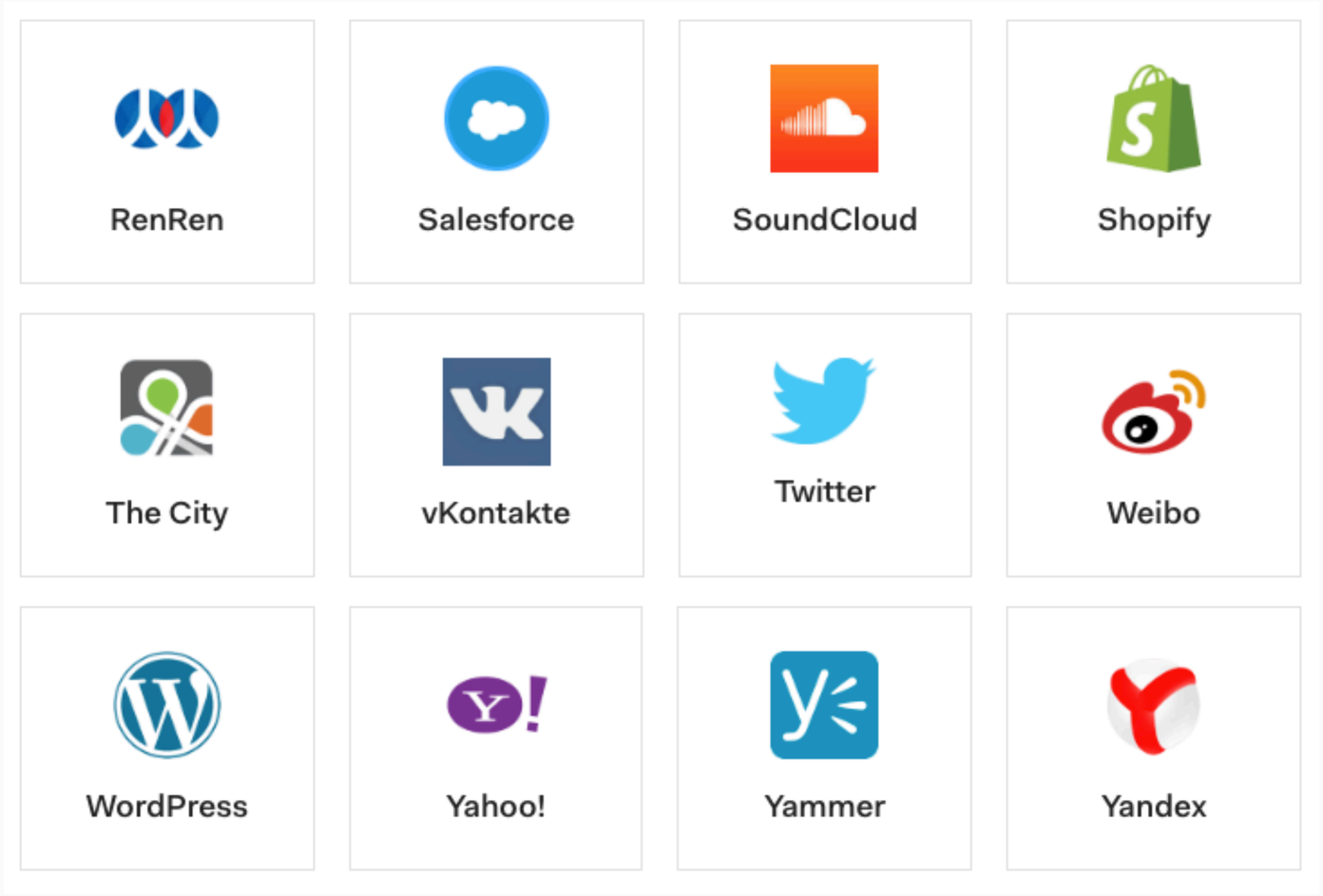
ORACLE Developer Champion

Federated Auth0



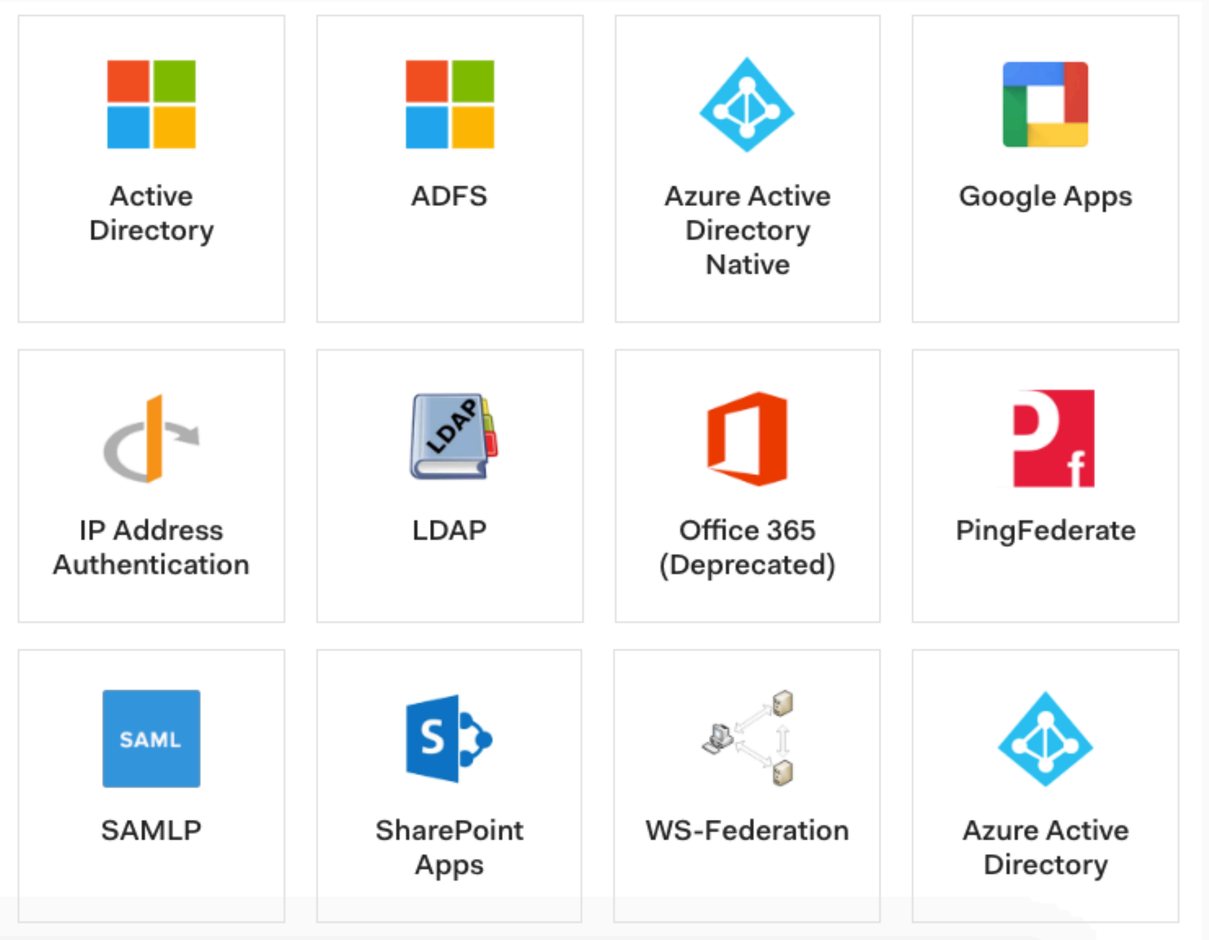
ORACLE Developer Champion

Federated Auth0



ORACLE Developer Champion

Federated Auth0



ORACLE Developer Champion

Federated Auth0

ORACLE Developer Champion

https://github.com/itrjwyss/Journey18

https://www.facebook.com/itrjwyss

@itrjwyss