Pragmatic Web Security

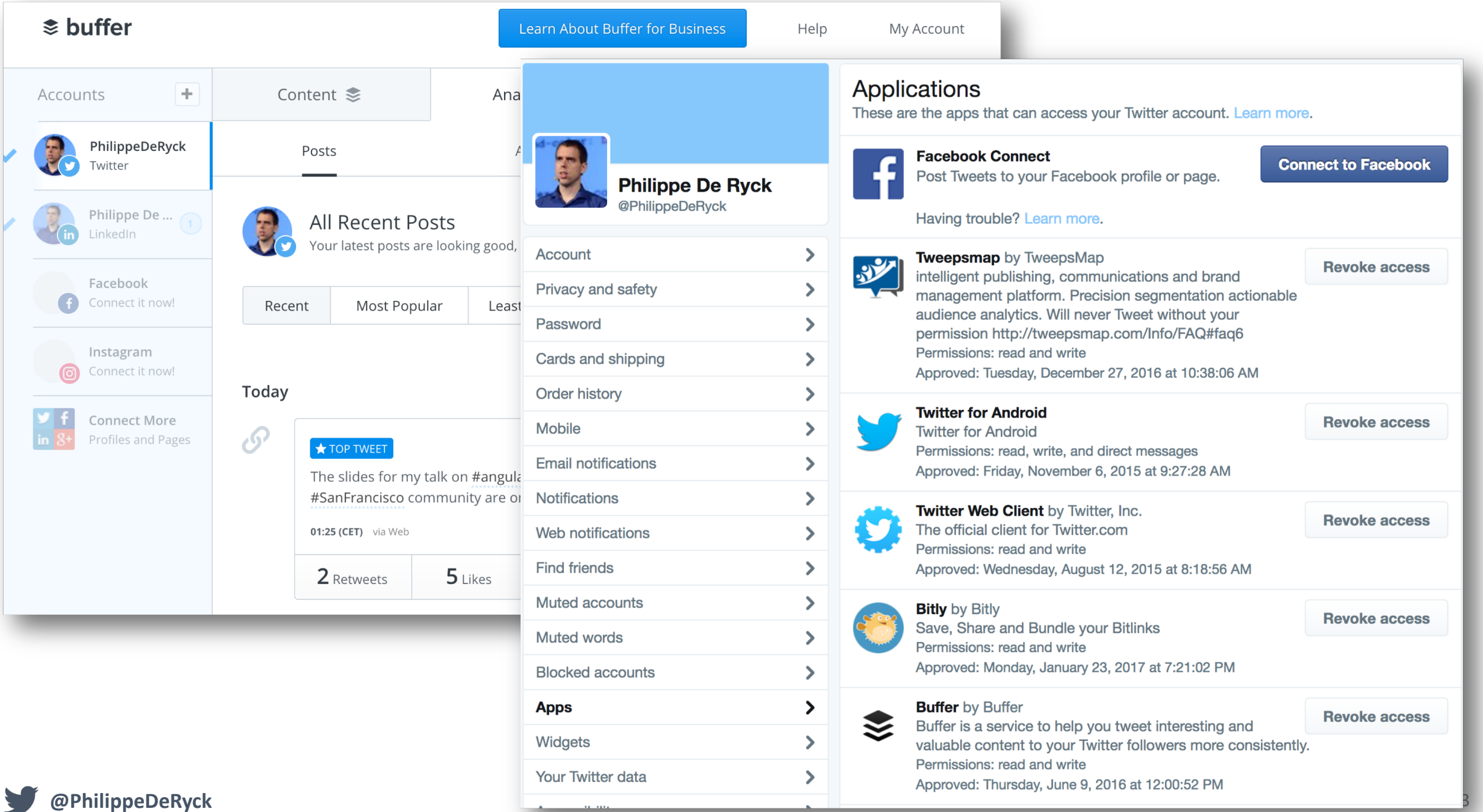
Security training for developers

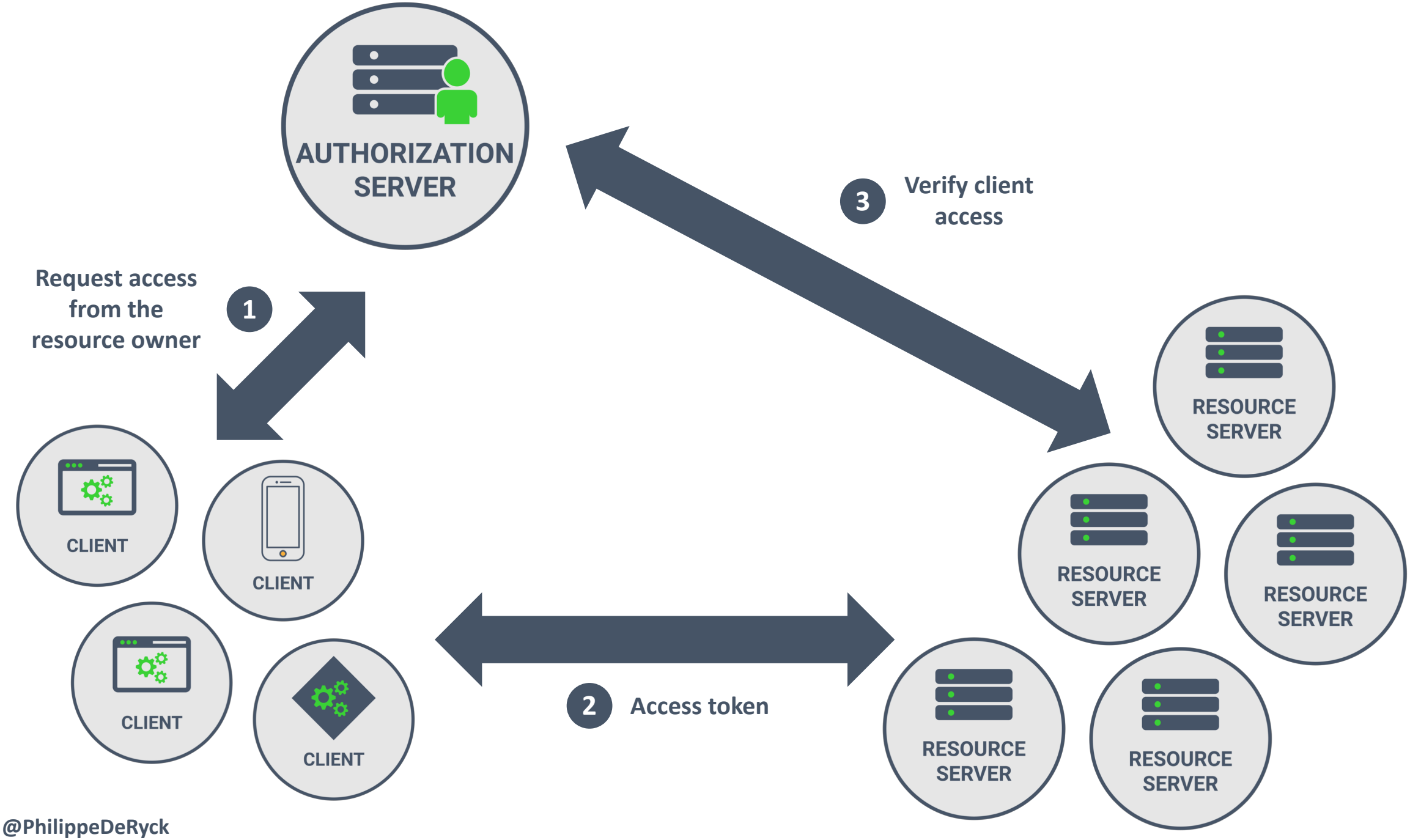
Introduction to OAuth 2.0 and OpenID Connect

Philippe De Ryck

@PhilippeDeRyck – philippe@PragmaticWebSecurity.com


Service
Voiturier 8 euros
dorr Paris
TAXI


buffer
Learn About Buffer for Business
Help
My Account
Accounts
Content
Ana
PhilippeDeRyck
Twitter
Philippe De ...
LinkedIn
Facebook
Connect it now!
Instagram
Connect it now!
Connect More
Profiles and Pages
Posts
All Recent Posts
Your latest posts are looking good,
Recent
Most Popular
Least
Today
TOP TWEET
The slides for my talk on #angula
#SanFrancisco community are o
01:25 (CET) via Web
2 Retweets
5 Likes
Philippe De Ryck
@PhilippeDeRyck
Account
Privacy and safety
Password
Cards and shipping
Order history
Mobile
Email notifications
Notifications
Web notifications
Find friends
Muted accounts
Muted words
Blocked accounts
Apps
Widgets
Your Twitter data
Applications
These are the apps that can access your Twitter account. Learn more.
Facebook Connect
Post Tweets to your Facebook profile or page.
Connect to Facebook
Having trouble? Learn more.
Tweepsmap by TweepsMap
intelligent publishing, communications and brand management platform. Precision segmentation actionable audience analytics. Will never Tweet without your permission http://tweepsmap.com/Info/FAQ#faq6
Permissions: read and write
Approved: Tuesday, December 27, 2016 at 10:38:06 AM
Revoke access
Twitter for Android
Twitter for Android
Permissions: read, write, and direct messages
Approved: Friday, November 6, 2015 at 9:27:28 AM
Revoke access
Twitter Web Client by Twitter, Inc.
The official client for Twitter.com
Permissions: read and write
Approved: Wednesday, August 12, 2015 at 8:18:56 AM
Revoke access
Bitly by Bitly
Save, Share and Bundle your Bitlinks
Permissions: read and write
Approved: Monday, January 23, 2017 at 7:21:02 PM
Revoke access
Buffer by Buffer
Buffer is a service to help you tweet interesting and valuable content to your Twitter followers more consistently.
Permissions: read and write
Approved: Thursday, June 9, 2016 at 12:00:52 PM
Revoke access


AUTHORIZATION SERVER
3
Verify client access
Request access from the resource owner
1
CLIENT
CLIENT
CLIENT
CLIENT
2
Access token
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER

- Traveling the world to deliver ***security courses***
  - In-depth web security training for developers
  - Custom training courses with developer-oriented labs
  - Covering web security, API security, Angular/React security

- 15+ years of security experience
  - Founder of **Pragmatic Web Security**
  - Author of ***Primer on client-side web security***
  - Creator of ***Web Security Fundamentals*** on edX

- Course curator of the **SecAppDev course**
  - Yearly security course targeted towards developers
  - More information on ***https://secappdev.org***

DR. PHILIPPE DE RYCK

PH.D. IN WEB SECURITY

GOOGLE DEVELOPER EXPERT

(NOT EMPLOYED BY GOOGLE)

OAuth 2.0

The client perspective

App details

The following app details will be visible to app users and are required to generate the API keys needed to authenticate Twitter developer products.

App name (required)

PragmaticWebSecurity

Maximum characters: **32**

Application description (required)

Share a description of your app. This description will be visible to users so this is a good place to tell them what your app does.

This is for personal use only, not for public use

Between 10 and 200 characters

Website URL (required)

https://pragmaticwebsecurity.com

Allow this application to be used to sign in with Twitter

Learn more

Enable Sign in with Twitter

Callback URLs

OAuth 1.0a applications should specify their oauth_callback URL on the request token step, which must match the URLs provided here. To restrict your application from using callbacks, leave these blank.

https://pragmaticwebsecurity.com/twittercallback.php

+Add another

Terms of Service URL

https://

Privacy policy URL

https://

Organization name

Organization website URL

https://

Tell us how this app will be used (required)

This field is only visible to Twitter employees. Help us understand how your app will be used. What will it enable you and your customers to do?

This is for personal use only, not for public use. Will be used as a relatable example of how OAuth 2.0 works in practice.

Cancel

Create

App details

The follo
to gener
products

App nam

Pragm

Applicat

Share a de
a good pla

This is

Website

https:/

Allow th
Learn m

Enab

Callback

OAuth 1.0
token step
applicatio

https://pragmaticwebsecurity.com/twittercallback.php

+Add another

Terms of Service URL

https://

Keys and tokens

Keys, secret keys and access tokens management.

Consumer API keys

QC1wPqVwsj74TCyqmEsdxXbJB (API key)

m80Rg66HLKck1SChuRUaKGBFwqZgCwysSGZDYT8nMlzXlGBNfM (API secret key)

Regenerate

Access token & access token secret

3417260589-WdGA0zLBXyc11BrACkBANpgSzpuhuHLK8JjfZhs (Access token)

JafkKM2wJwjrMrT6GwSfJoHW42Yd0aVXG4crmX3ZmqhXq (Access token secret)

Read and write (Access level)

Revoke

Regenerate

Don't worry, these are revoked!

Cancel

Create

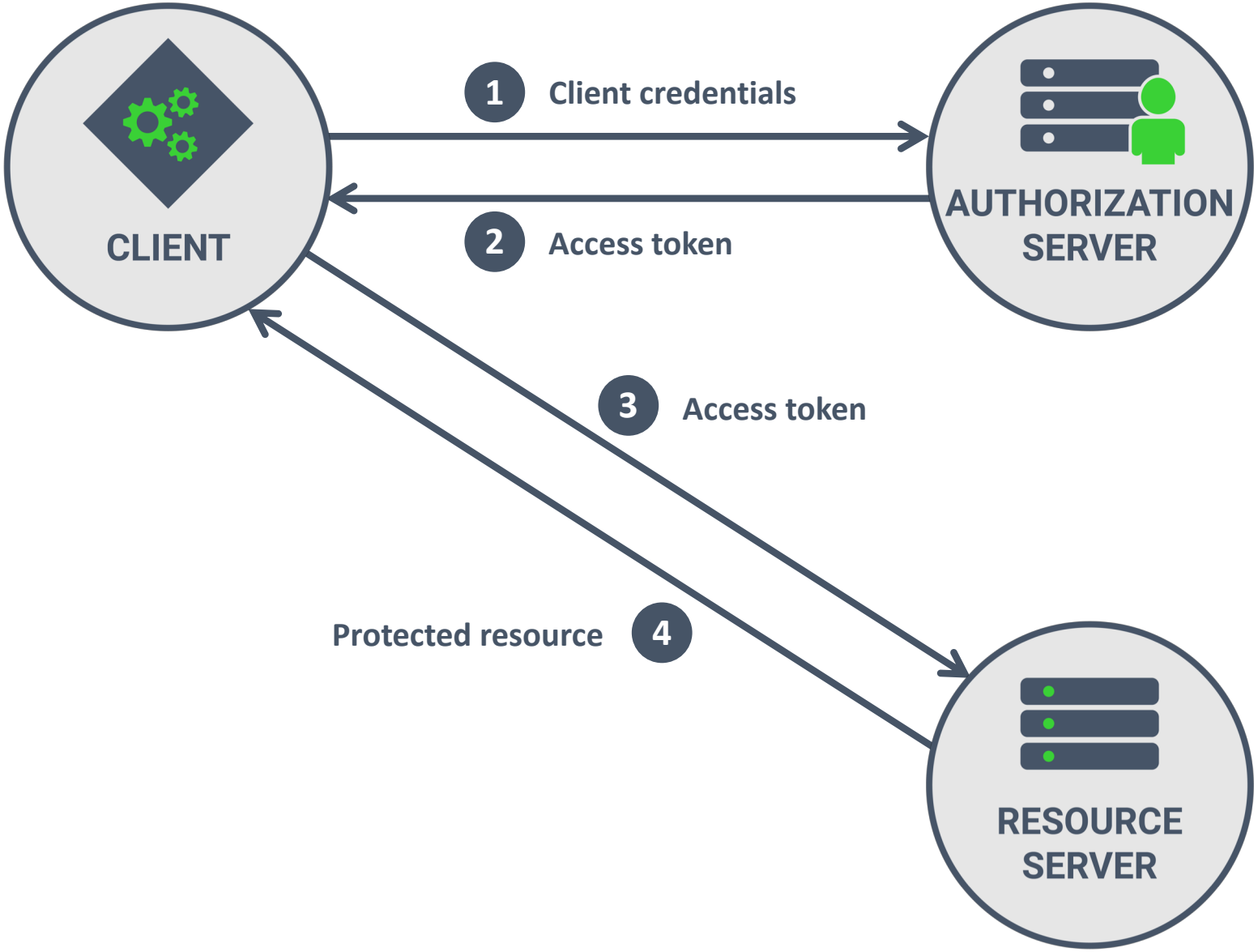
Scenario 1 – Show a selected number of tweets

Almost every application depends on authentication, a much-debated topic. Who better to teach about it than @jimfenton, the co-editor of the #NIST SP 800-63 Digital Identity Guidelines. Proud to have Jim on board. buff.ly/1Ric8Zq

For the 15th year in a row, Bart Preneel from @CosicBe will be at SecAppDev. He is one of the world's experts on cryptography. This year, he will teach about crypto, but will also give his expert opinion on #blockchain and the current hype. buff.ly/1Ric8Zq

With a lot of excitement, we can announce @jimmesta will be part of the SecAppDev 2019 faculty. He is one of the top experts on security in DevOps environments. He also teaches one of his excellent 1-day workshops, where you dive #Kubernetes! buff.ly/1Ric8Zq

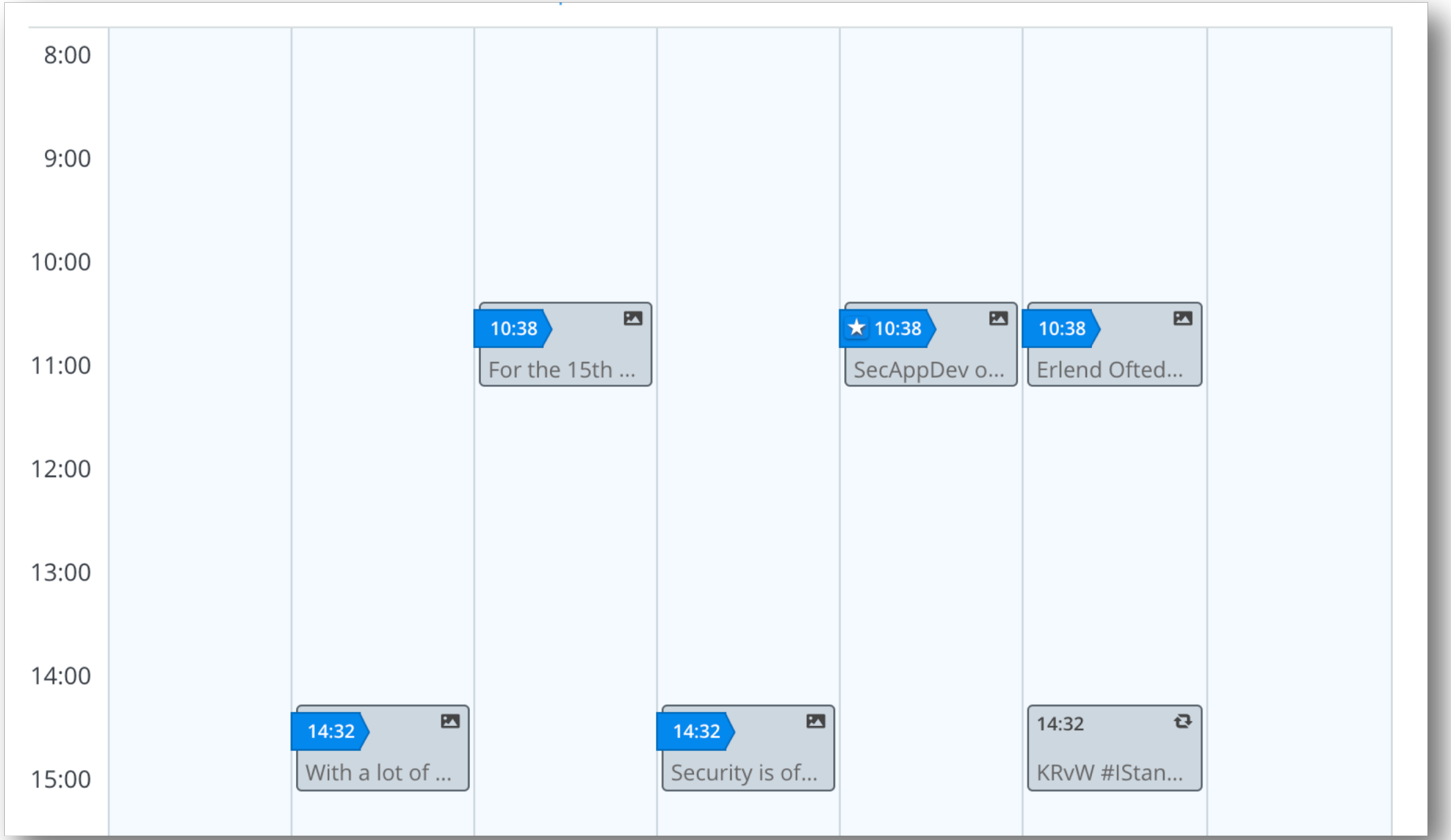
The Client Credentials Grant flow



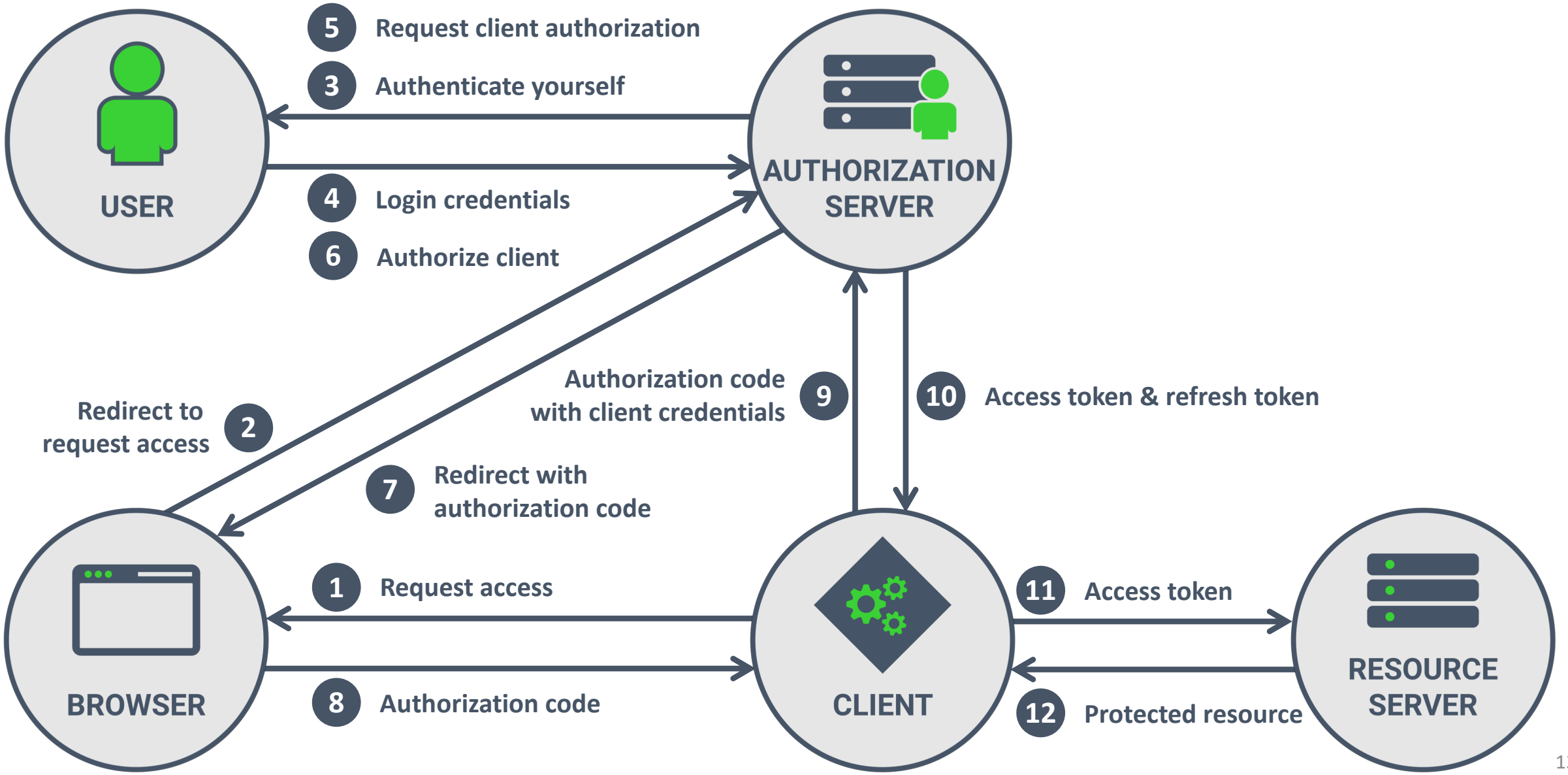
Client credentials grant

- Direct access by the client application
- Access token obtained using client credentials

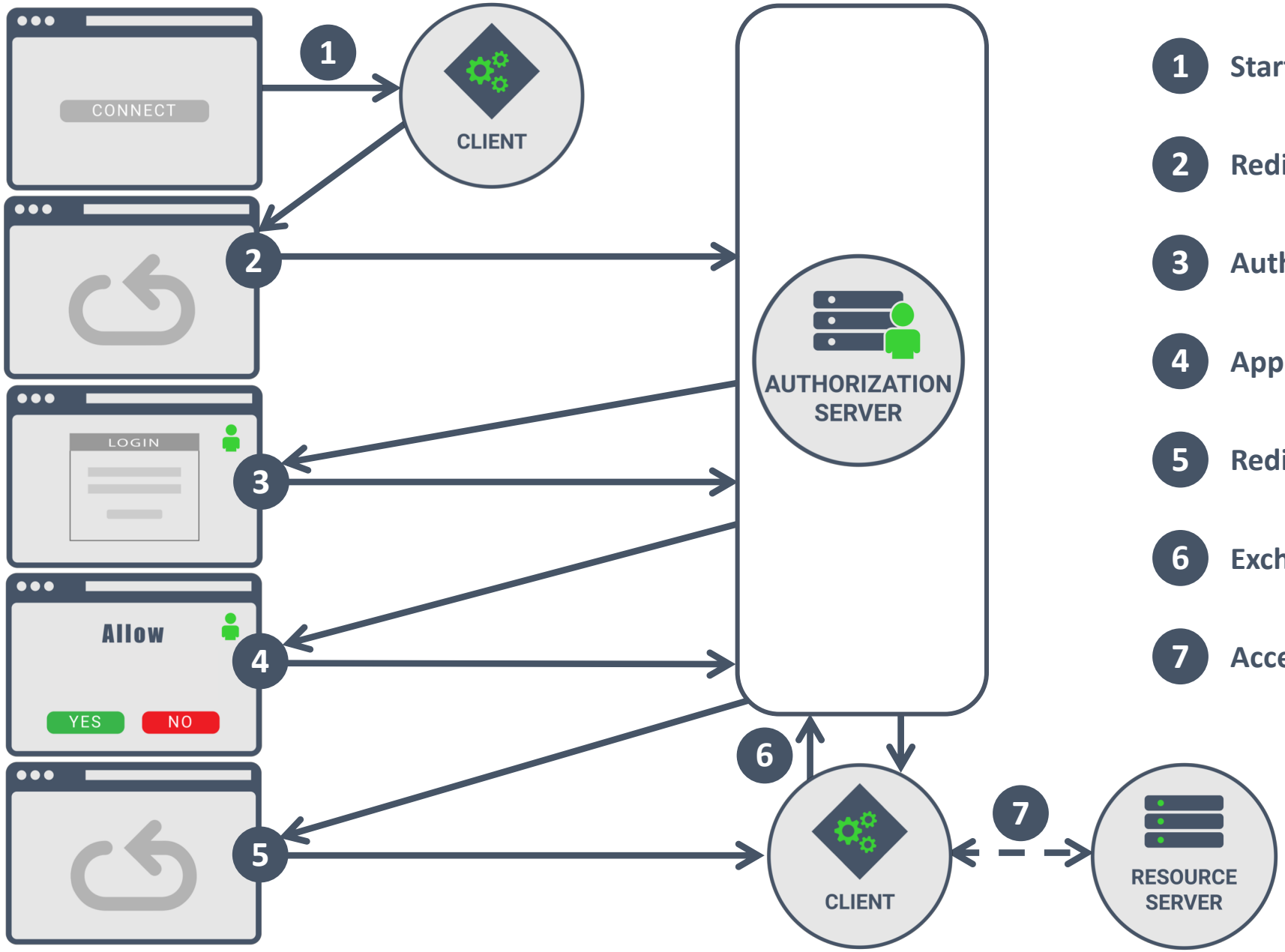
Scenario 2 – Schedule tweets on behalf of a user



The Authorization Code Grant flow



The Authorization Code Grant flow



1. Start the delegation process
2. Redirect to the authorization server
3. Authenticate the user
4. Approve access delegation
5. Redirect with authorization code
6. Exchange code for access token
7. Access protected resources

Requesting an authorization code

```
https://twitter.example.com/auth
  ?response_type=code
  &client_id=PragmaticWebSecurity
  &scope=read write
  &redirect_uri=https://pragmatic…/twittercallback.php
  &state=s0wzojm2w8c23xzprkk6
```

Response containing authorization code

```
https://pragmatic…/twittercallback.php
  ?code=eyJhb...0X4UeQ
  &state=s0wzojm2w8c23xzprkk6
```

Requesting an access token

```
POST /auth
Authorization: Basic UmFuZG9tQ2xpZW50SU...tODdlYTJmZDVhN2Rm
Host: twitter.example.com

 grant_type=authorization_code
&redirect_uri=https%3A%2F%2Fpragmaticweb…%2Ftwittercallback.php
&client_id=PragmaticWebSecurity
&code=eyJhb...0X4UeQ
```

Response containing access token

```
{
    "access_token": "eyJhbGciO...du6TY9w",
    "expires_in": 300,
    "token_type": "bearer"
    "refresh_token": "eyJhbGciO...E4wRw",
}
```

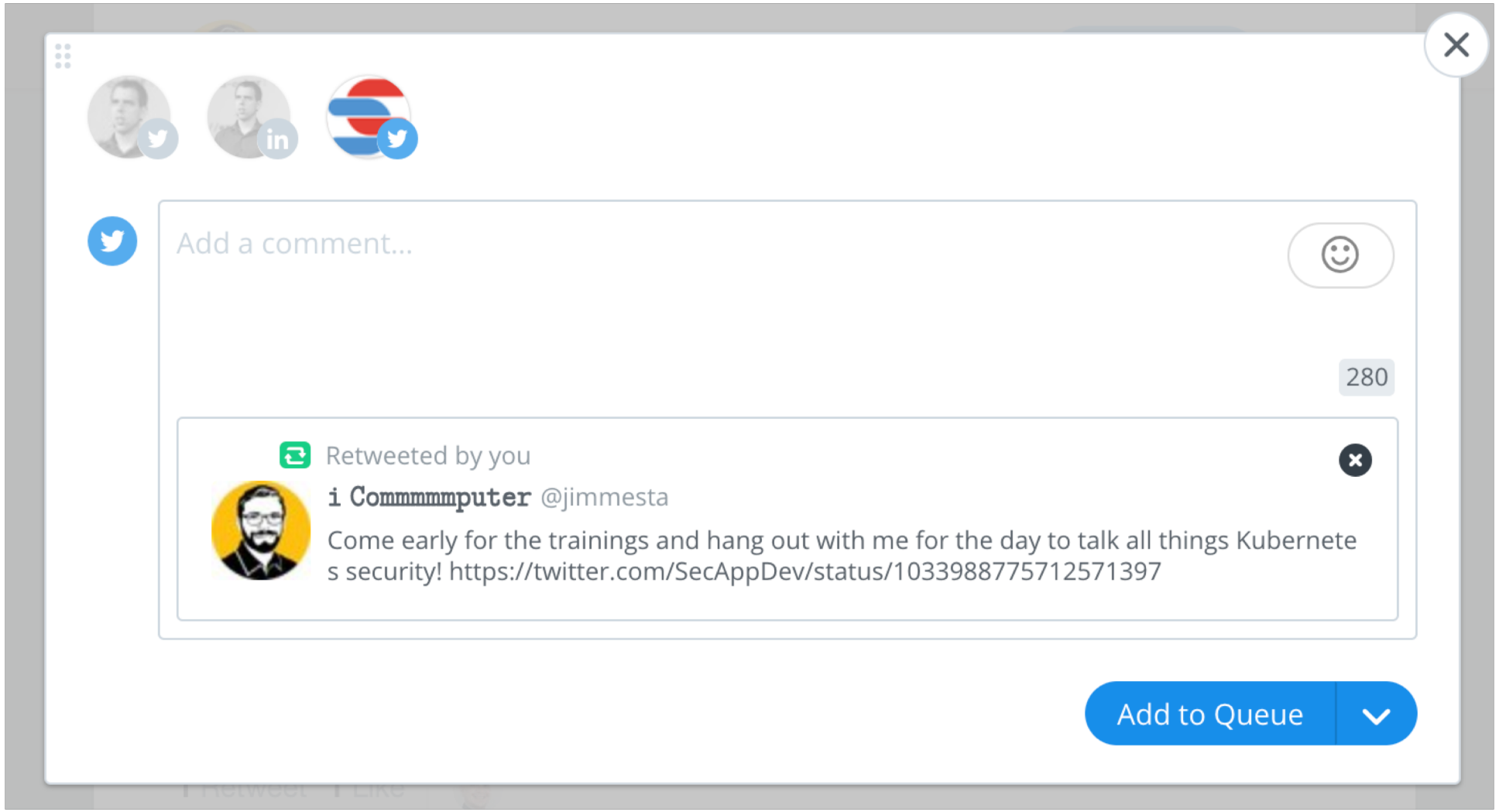
Client credentials grant

- Direct access by the client application
- Access token obtained using client credentials

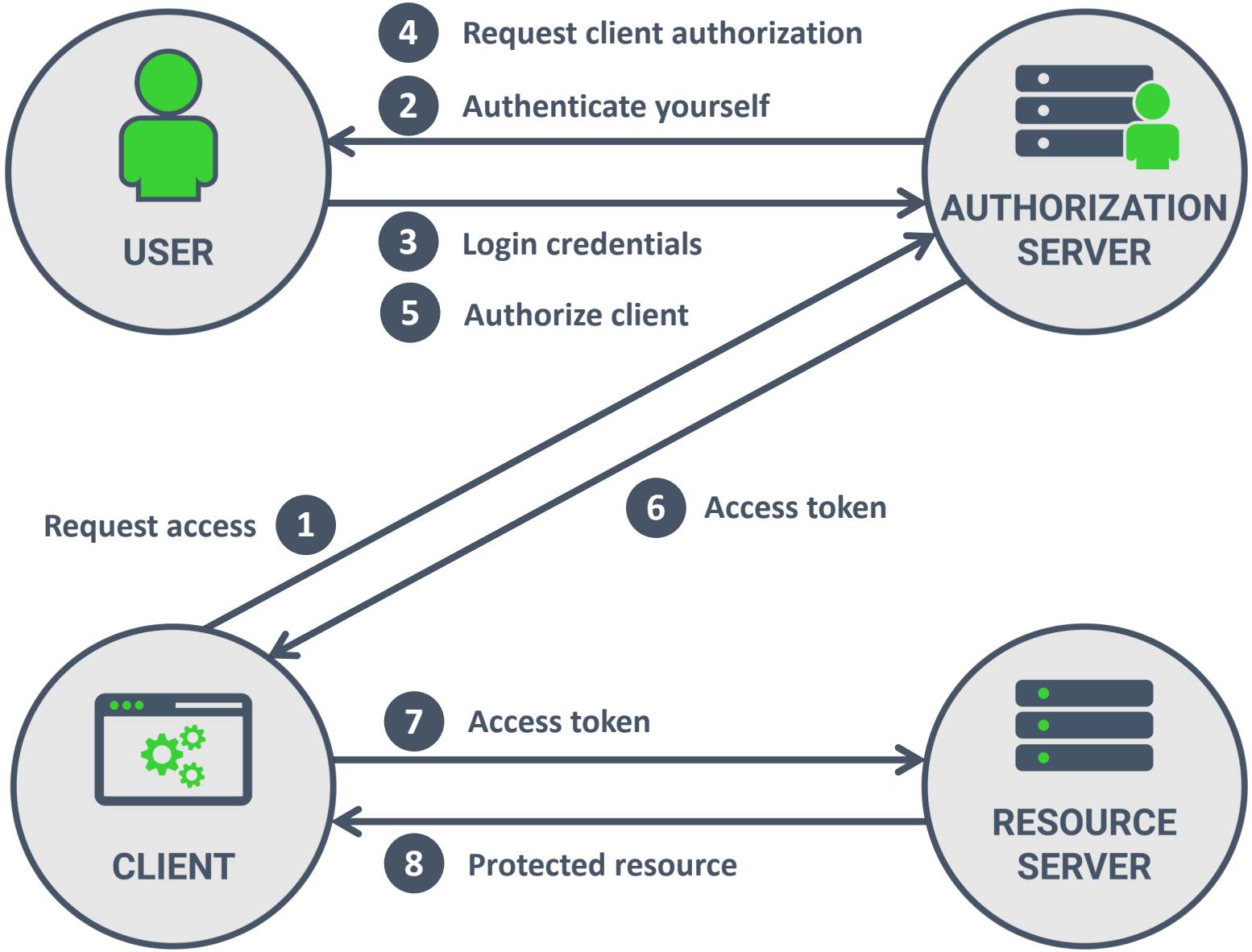
Authorization code grant

- Delegated access to a backend application
- Access token obtained by exchanging code with client credentials
- Refresh token can be used with client credentials

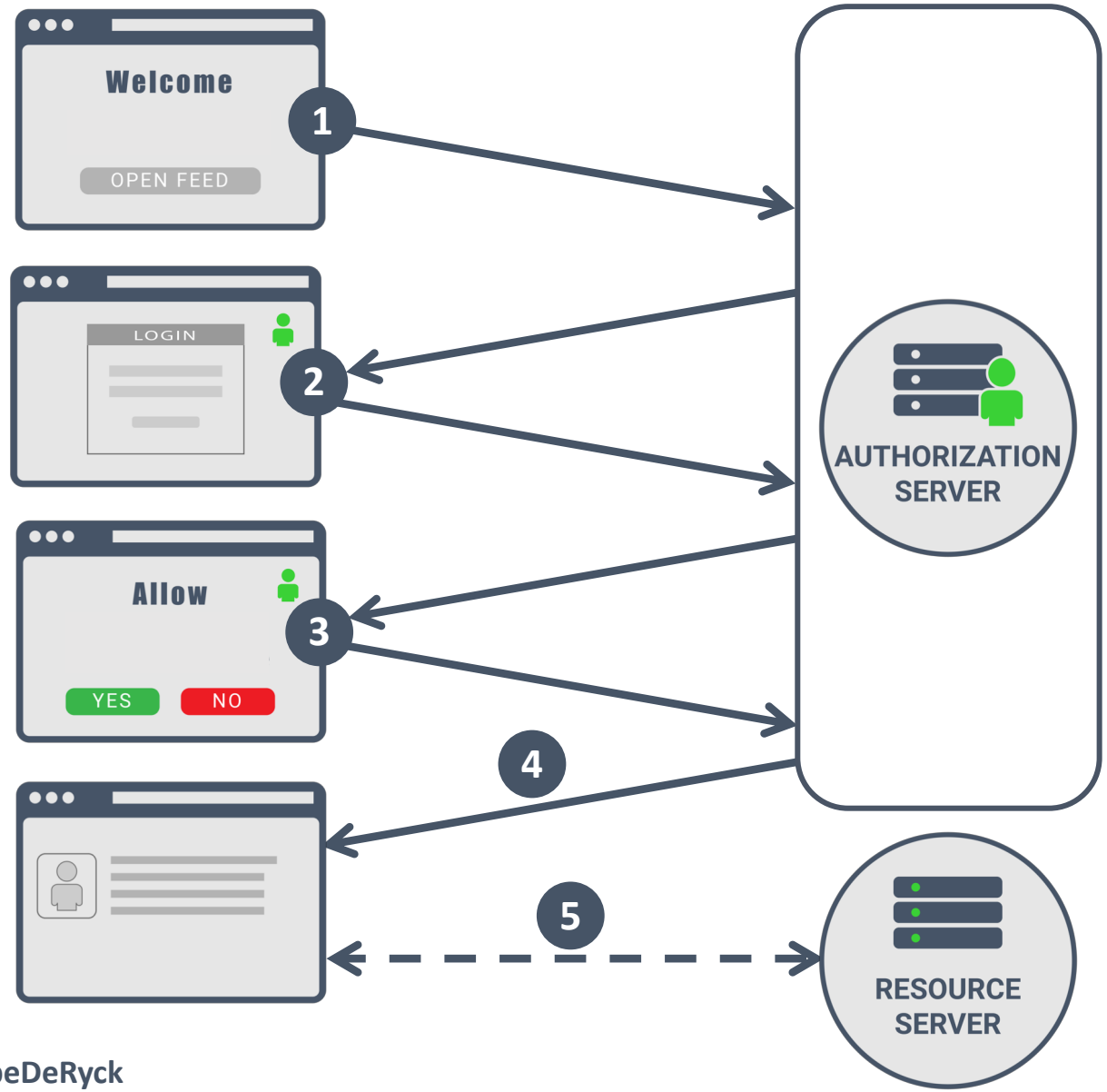
SCENARIO 3 – ALLOW LIVE INTERACTION ON BEHALF OF A USER



THE IMPLICIT GRANT FLOW



The Implicit Grant flow



1. Start the delegation process
2. Authenticate the user
3. Approve access delegation
4. Load callback with access token
5. Access protected resources

Requesting an access token

```
https://twitter.example.com/auth
   ?response_type=token
   &client_id=PragmaticWebSecurity
   &scope=read write
   &redirect_uri=https://pragmatic…/twittercallback.php
   &state=s0wzojm2w8c23xzprkk6
```

Response containing access token

```
https://pragmatic…/twittercallback.php
   #access_token=eyJhb...0X4UeQ
   &token_type=bearer
   &expires_in=300
   &state=s0wzojm2w8c23xzprkk6
```

Client credentials grant

- Direct access by the client application
- Access token obtained using client credentials

Authorization code grant

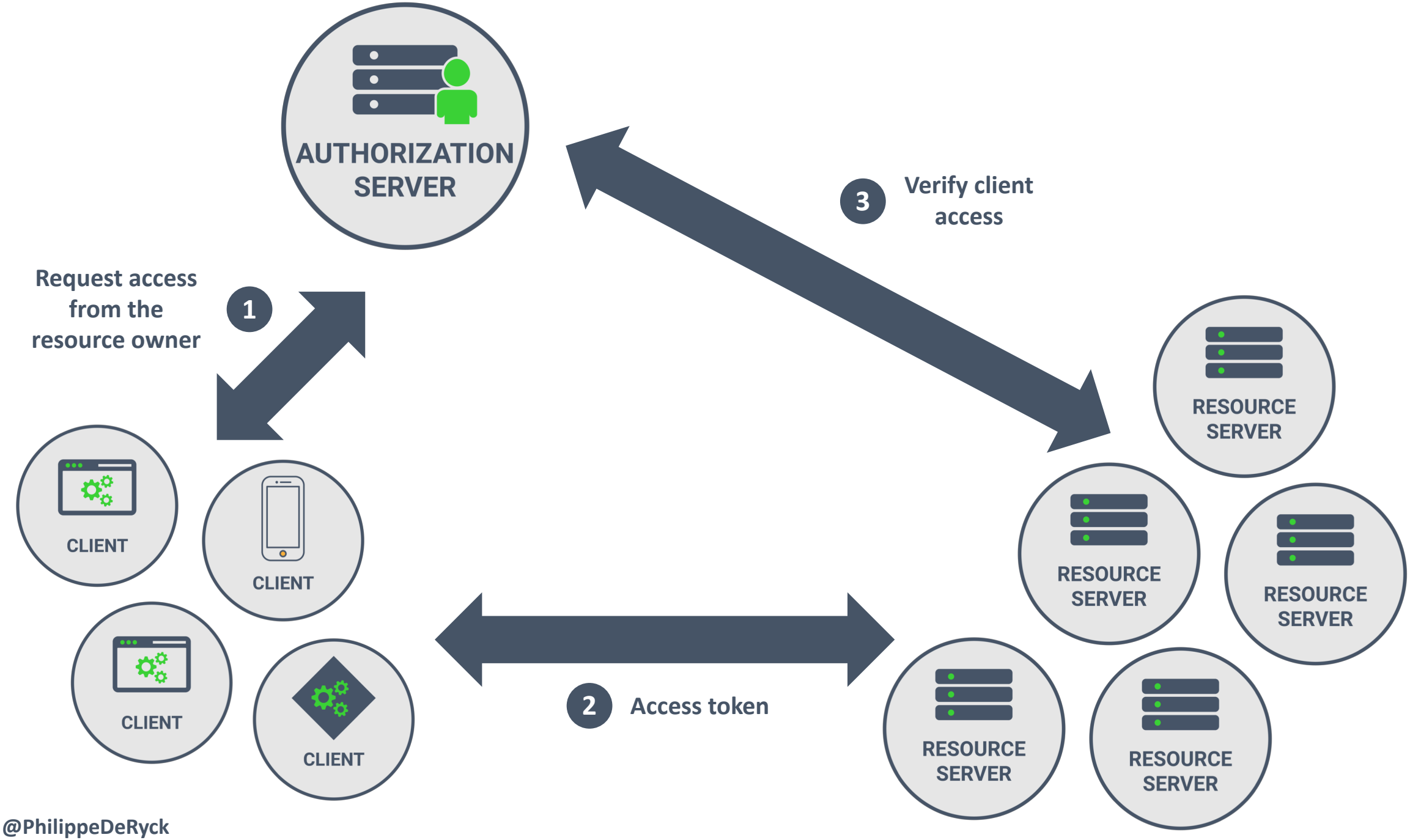
- Delegated access to a backend application
- Access token obtained by exchanging code with client credentials
- Refresh token can be used with client credentials

Implicit grant

- Delegated access to a frontend application
- Access token directly obtained through the redirect
- Not supposed to have access to refresh tokens

OAuth 2.0

The resource server's perspective


AUTHORIZATION SERVER
Request access from the resource owner
1
3
Verify client access
CLIENT
CLIENT
CLIENT
CLIENT
2
Access token
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER
RESOURCE SERVER

To the client, an access token might just as well be a dinosaur

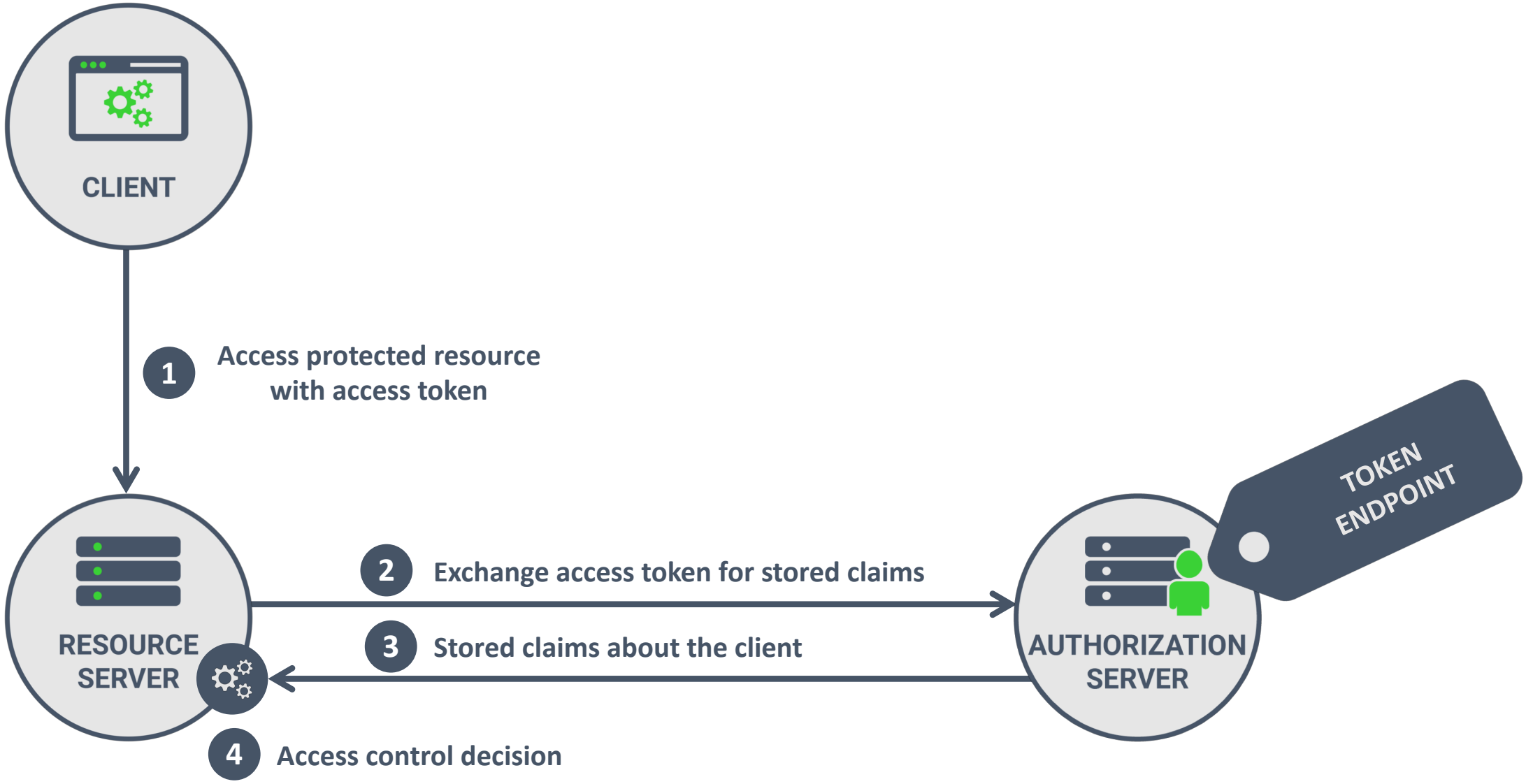
```
2YotnFZFEjr1zCsicMWpAA
```

```
eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJqZG9lQGV4YW1wbGUuY29tIiwi
  YXVkIjoiaHR0cHM6Ly9hcGkuZXhhbXBsZS5jb20iLCJhenAiOiJSY
W5kb21DbGllbnRJRCIsImlzcyI6Imh0dHBzOi8vYXV0aG9yaXphdGlvbn
  NlcnZlci5leGFtcGxlLmNvbS8iLCJleHAiOjE0MTkzNTYyMzgsIml
hdCI6MTQxOTM1MDIzOCwic2NvcGUiOiJyZWFkIHdyaXRlIiwianRpIjoi
  NDA1YjRkNGUtODUwMS00ZTFhLWExMzgtZWQ4NDU1Y2QxZDQ3In0.
  FCk3Wo8DnFEHb02JCd9BWAHQ48BBt3n2YLQV6TpLMpFvTRNCZJAA-
 aEH4LrE7oVejvGd7YWGDy2Vzb7x-Bpg7yMYxozUerCkMy_F4Iw_xctgE
  J3WF_TTJFhISGNoWlFXspM5d9EQvMvk0JxAovhE0HfXv5GCosGy-
 0oT7ShQrwZLBIwE9d0ceUcmly42dvDZSsqHDIzPjrFzvpXwbZqq_sRFnh
 6MHlmmug7t1UCs85caoLhfSweaT0z7ED8P2Tsg_HgmnaaeDapszG6Lcke
  BglqYwbRHy6X6LAcJfAkkwAlqrU0Vu4azsuE8BsLPKMYzu9ZeCoH
  dLHYdtz-I0yKQ
```

2YotnFZFEjr1zCsicMWpAA


```
eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJqZG9lQGV4YW1wbGUuY29tIiwi
  YXVkIjoiaHR0cHM6Ly9hcGkuZXhhbXBsZS5jb20iLCJhenAiOiJSY
W5kb21DbGllbnRJRCIsImlzcyI6Imh0dHBzOi8vYXV0aG9yaXphdGlvbn
  NlcnZlci5leGFtcGxlLmNvbS8iLCJleHAiOjE0MTkzNTYyMzgsIml
hdCI6MTQxOTM1MDIzOCwic2NvcGUiOiJyZWFkIHdyaXRlIiwianRpIjoi
  NDA1YjRkNGUtODUwMS00ZTFhLWExMzgtZWQ4NDU1Y2QxZDQ3In0.
  FCk3Wo8DnFEHb02JCd9BWAHQ48BBt3n2YLQV6TpLMpFvTRNCZJAA-
 aEH4LrE7oVejvGd7YWGDy2Vzb7x-Bpg7yMYxozUerCkMy_F4Iw_xctgE
  J3WF_TTJFhISGNoWlFXspM5d9EQvMvk0JxAovhE0HfXv5GCosGy-
 0oT7ShQrwZLBIwE9d0ceUcmly42dvDZSsqHDIzPjrFzvpXwbZqq_sRFnh
 6MHlmmug7t1UCs85caoLhfSweaT0z7ED8P2Tsg_HgmnaaeDapszG6Lcke
  BglqYwbRHy6X6LAcJfAkkwAlqrU0Vu4azsuE8BsLPKMYzu9ZeCoH
  dLHYdtz-I0yKQ
```

TOKEN INTROSPECTION FOR REFERENCE TOKENS



Token introspection request

```
POST /token_info
Authorization: Bearer eyJhb...N2Rm
Host: twitter.example.com

 token=2YotnFZFEjr1zCsicMWpAA
&token_type_hint=access_token
```

Token introspection response

```
{
    "active": true
    "client_id": "PragmaticWebSecurity",
    "sub": "Z5O3upPC88QrAjx00dis"
    "exp": 1419356238,
    "scope": "read write"
}
```

Reference tokens

- An identifier pointing to metadata kept by the authorization server
- Authorization server retains full control over the metadata
- Require a backchannel request when received by the resource server
- Easy to revoke if needed

```
2YotnFZFEjr1zCsicMWpAA
```

```
eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJqZG9lQGV4YW1wbGUuY29tIiwi
YXVkIjoiaHR0cHM6Ly9hcGkuZXhhbXBsZS5jb20iLCJhenAiOiJSY
W5kb21DbGllbnRJRCIsImlzcyI6Imh0dHBzOi8vYXV0aG9yaXphdGlvbn
NlcnZlci5leGFtcGxlLmNvbS8iLCJleHAiOjE0MTkzNTYyMzgsIml
hdCI6MTQxOTM1MDIzOCwic2NvcGUiOiJyZWFkIHdyaXRlIiwianRpIjoi
NDA1YjRkNGUtODUwMS00ZTFhLWExMzgtZWQ4NDU1Y2QxZDQ3In0.
FCk3Wo8DnFEHb02JCd9BWAHQ48BBt3n2YLQV6TpLMpFvTRNCZJAA-
aEH4LrE7oVejvGd7YWGDy2Vzb7x-Bpg7yMYxozUerCkMy_F4Iw_xctgE
J3WF_TTJFhISGNoWlFXspM5d9EQvMvk0JxAovhE0HfXv5GCosGy-
0oT7ShQrwZLBIwE9d0ceUcmly42dvDZSsqHDIzPjrFzvpXwbZqq_sRFnh
6MHlmmug7t1UCs85caoLhfSweaT0z7ED8P2Tsg_HgmnaaeDapszG6Lcke
BglqYwbRHy6X6LAcJfAkkwAlqrU0Vu4azsuE8BsLPKMYzu9ZeCoH
dLHYdtz-I0yKQ
```

PAYLOAD: DATA


```
{
  "sub": "philippe@secappdev.org",
  "aud": "https://pragmaticwebsecurity.com",
  "azp": "PragmaticWebSecurity",
  "iss": "https://twitter.example.com/",
  "exp": 1419356238,
  "iat": 1419350238,
  "scope": "read write",
  "jti": "405b4d4e-8501-4e1a-a138-ed8455cd1d47"
}
```

Reference tokens

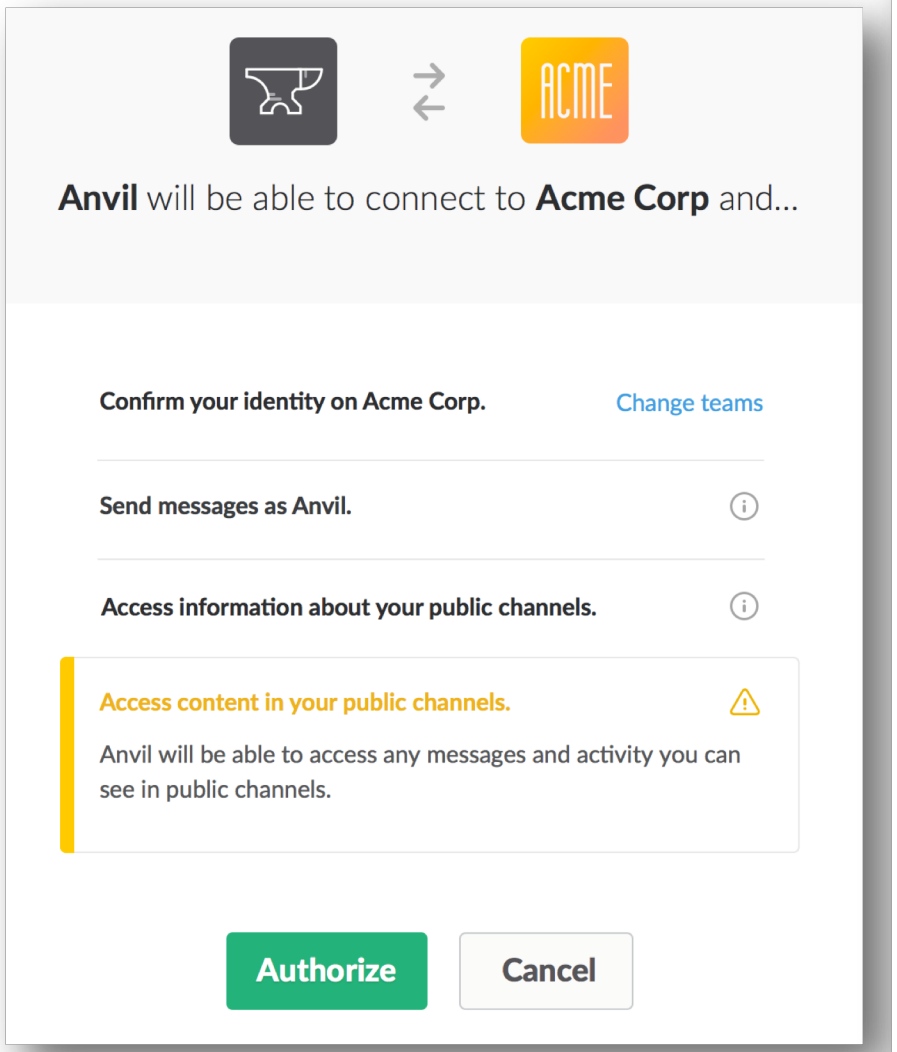
- An identifier pointing to metadata kept by the authorization server
- Authorization server retains full control over the metadata
- Require a backchannel request when received by the resource server
- Easy to revoke if needed

Self-contained tokens

- The token itself contains the metadata used by the authorization server
- Stored on the client, so out of reach from the authorization server
- Can be used independently by the resource server AFTER INTEGRITY CHECK
- Hard or impossible to revoke

scope=read write

Scopes as used by the Slack API



OAuth Scope	Associated Methods	
`channels:history`	channels.history	channels.replies
`channels:read`	channels.info	channels.list
`channels:write`	channels.archive channels.create channels.invite channels.join channels.kick channels.leave	channels.mark channels.rename channels.setPurpose channels.setTopic channels.unarchive conversations.join
`chat:write:bot`	chat.delete chat.postEphemeral	chat.postMessage chat.update
`chat:write:user`	chat.delete chat.meMessage chat.postEphemeral	chat.postMessage chat.update

Scopes as used by the Google API

Google Analytics API, v3

Scopes	
https://www.googleapis.com/auth/analytics	View and manage your Google Analytics data
https://www.googleapis.com/auth/analytics.edit	Edit Google Analytics management entities
https://www.googleapis.com/auth/analytics.manage.users	Manage Google Analytics Account users by email address
https://www.googleapis.com/auth/analytics.manage.users.readonly	View Google Analytics user permissions
https://www.googleapis.com/auth/analytics.provision	Create a new Google Analytics account along with its default property and view
https://www.googleapis.com/auth/analytics.readonly	View your Google Analytics data
https://www.googleapis.com/auth/analytics.user.deletion	Manage Google Analytics user deletion requests

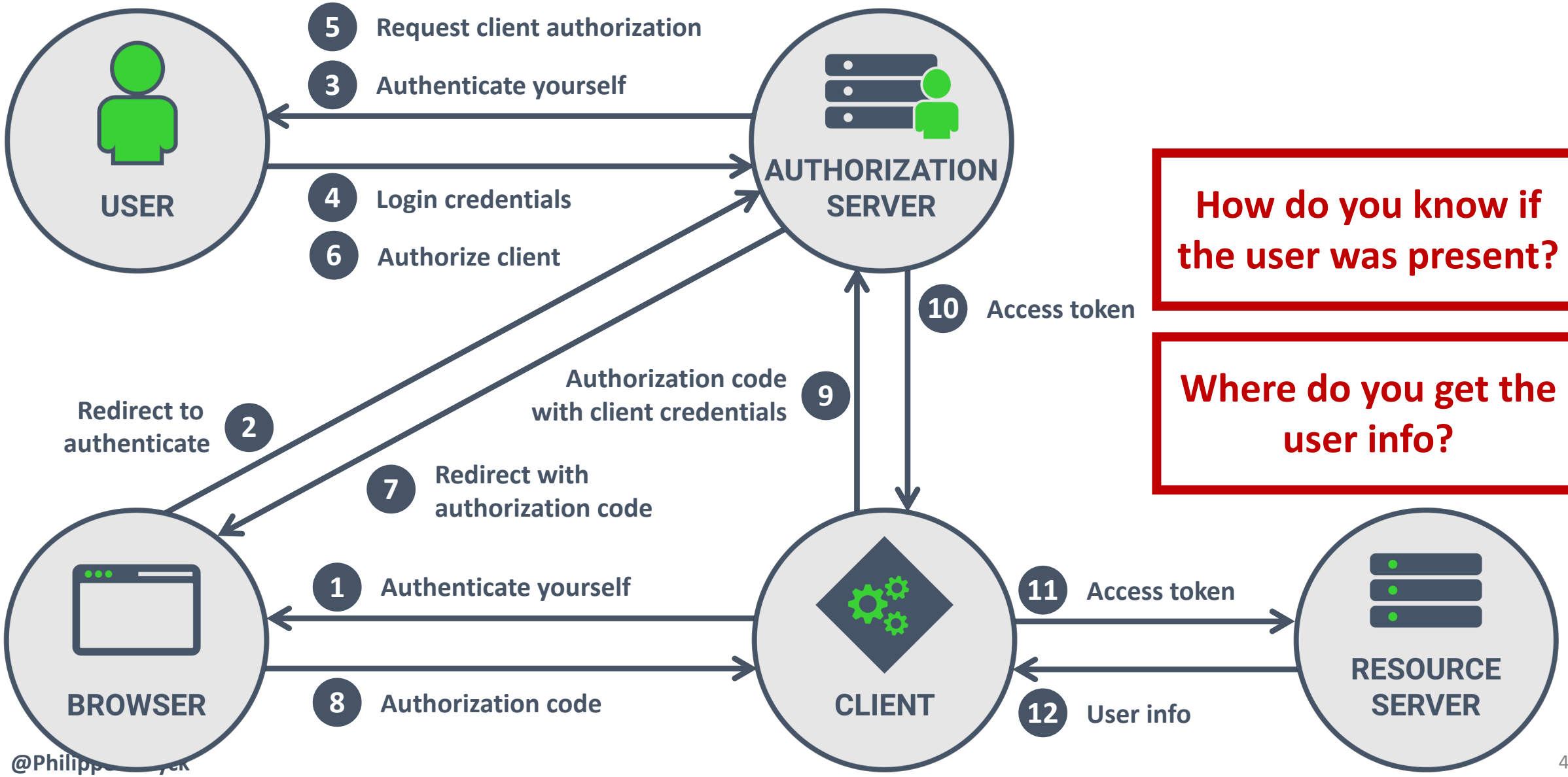
Analytics Reporting API, v4

Scopes	
https://www.googleapis.com/auth/analytics	View and manage your Google Analytics data
https://www.googleapis.com/auth/analytics.readonly	View your Google Analytics data

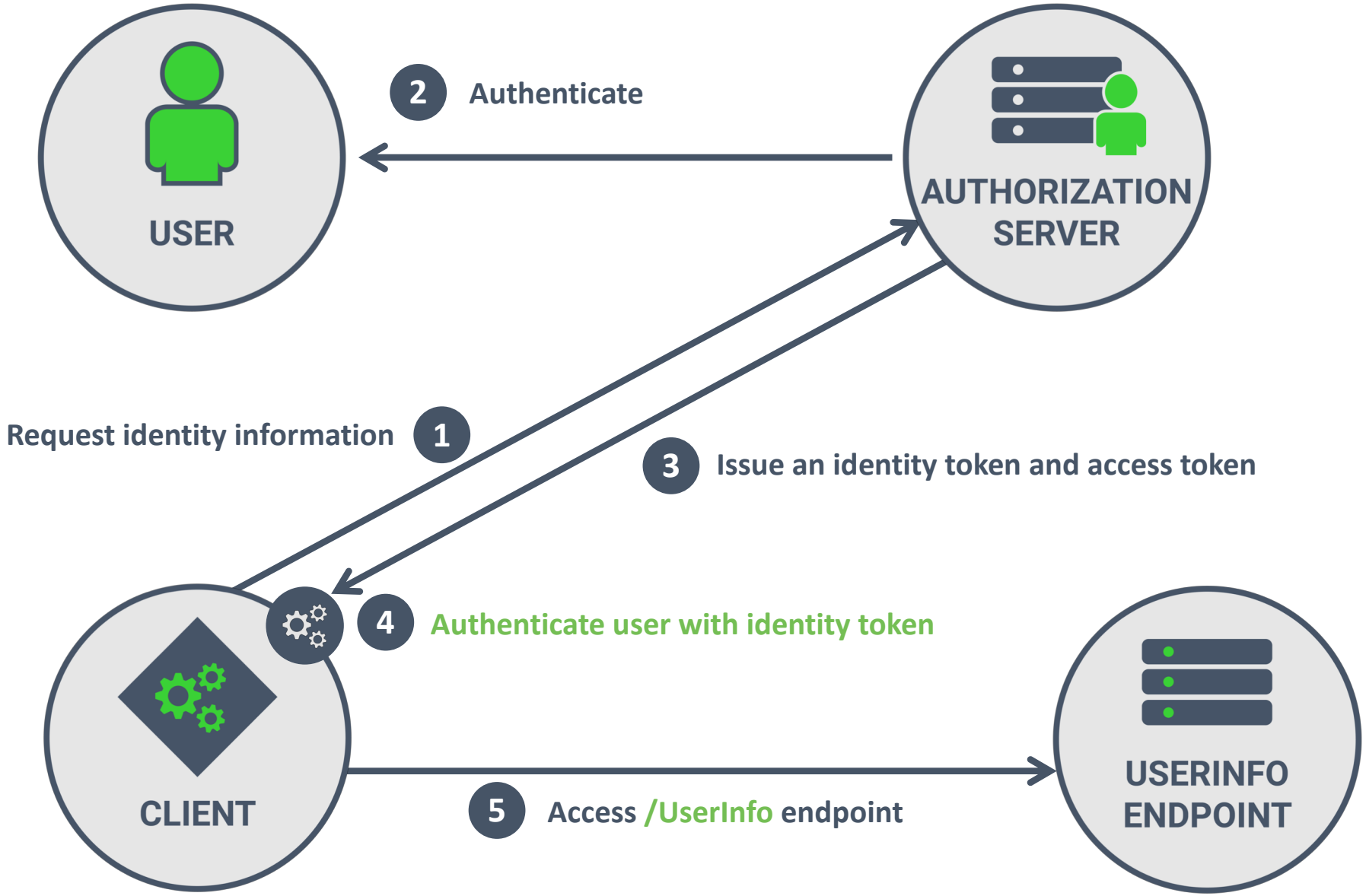
OpenID Connect

Authentication with OAuth 2.0

PSEUDO-AUTHENTICATION WITH OAUTH 2.0



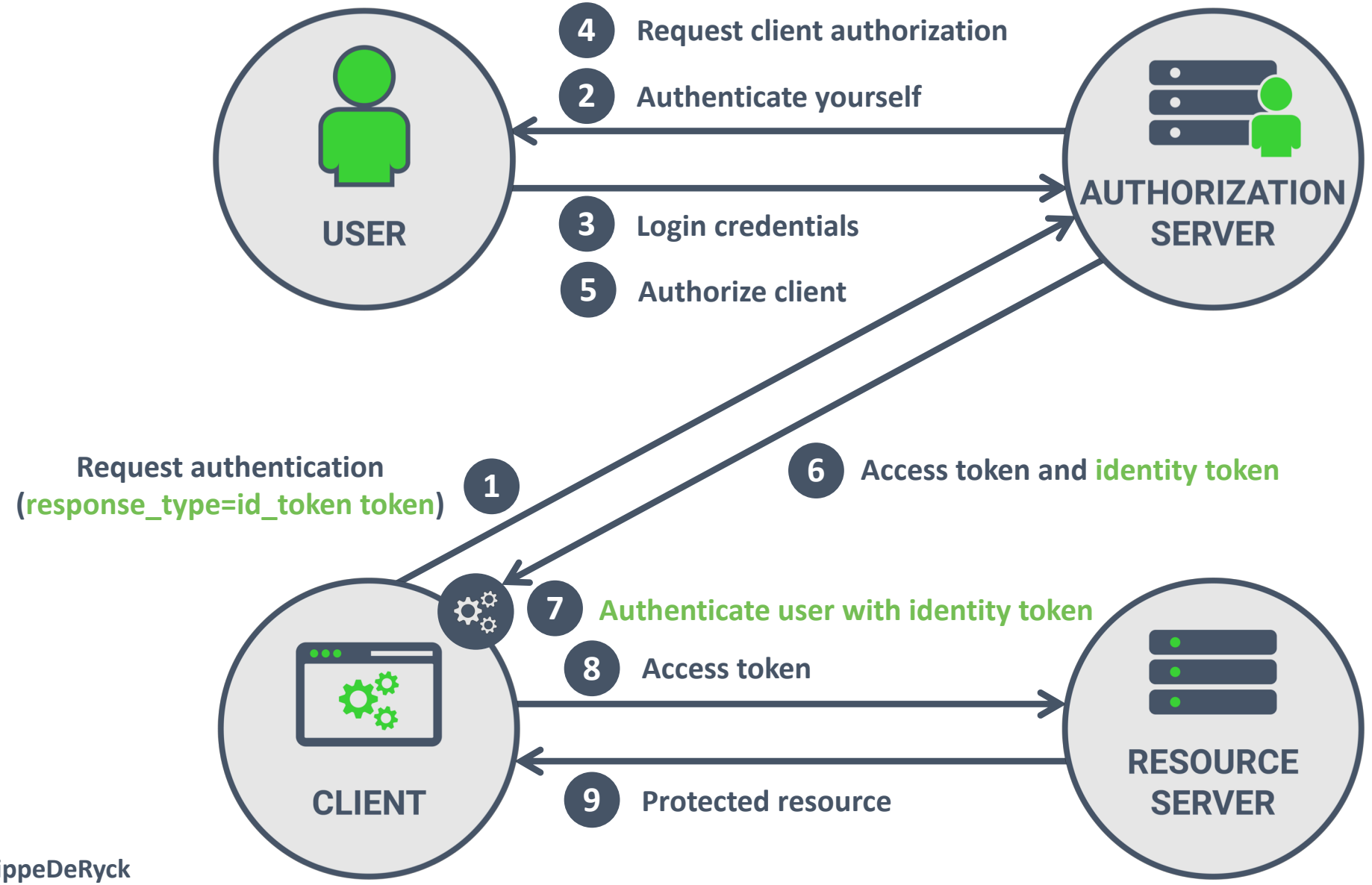
Conceptual overview of OpenID Connect



PAYLOAD: DATA


```
{
  "jti": "10368e39-55a4-4438-862a-3eec111cce72",
  "exp": 1535316231,
  "nbf": 0,
  "iat": 1535309031,
  "iss":
"https://keycloak.restograde.com/auth/realms/Restograde",
  "aud": "com.restograde.reviewer",
  "sub": "eb88c689-5f33-43a2-b990-3510b58a4bae",
  "typ": "ID",
  "azp": "com.restograde.reviewer",
  "nonce": "",
  "auth_time": 1535308479,
  "session_state": "55a83b93-fab7-4360-8869-eea9df0ff353",
  "at_hash": "iaTesTySu4X6VZT7a2ic-A",
  "acr": "0",
  "email_verified": false,
  "name": "Philippe De Ryck",
  "preferred_username": "philippe",
  "given_name": "Philippe",
  "family_name": "De Ryck",
  "email": "philippe@pragmaticwebsecurity.com"
}
```

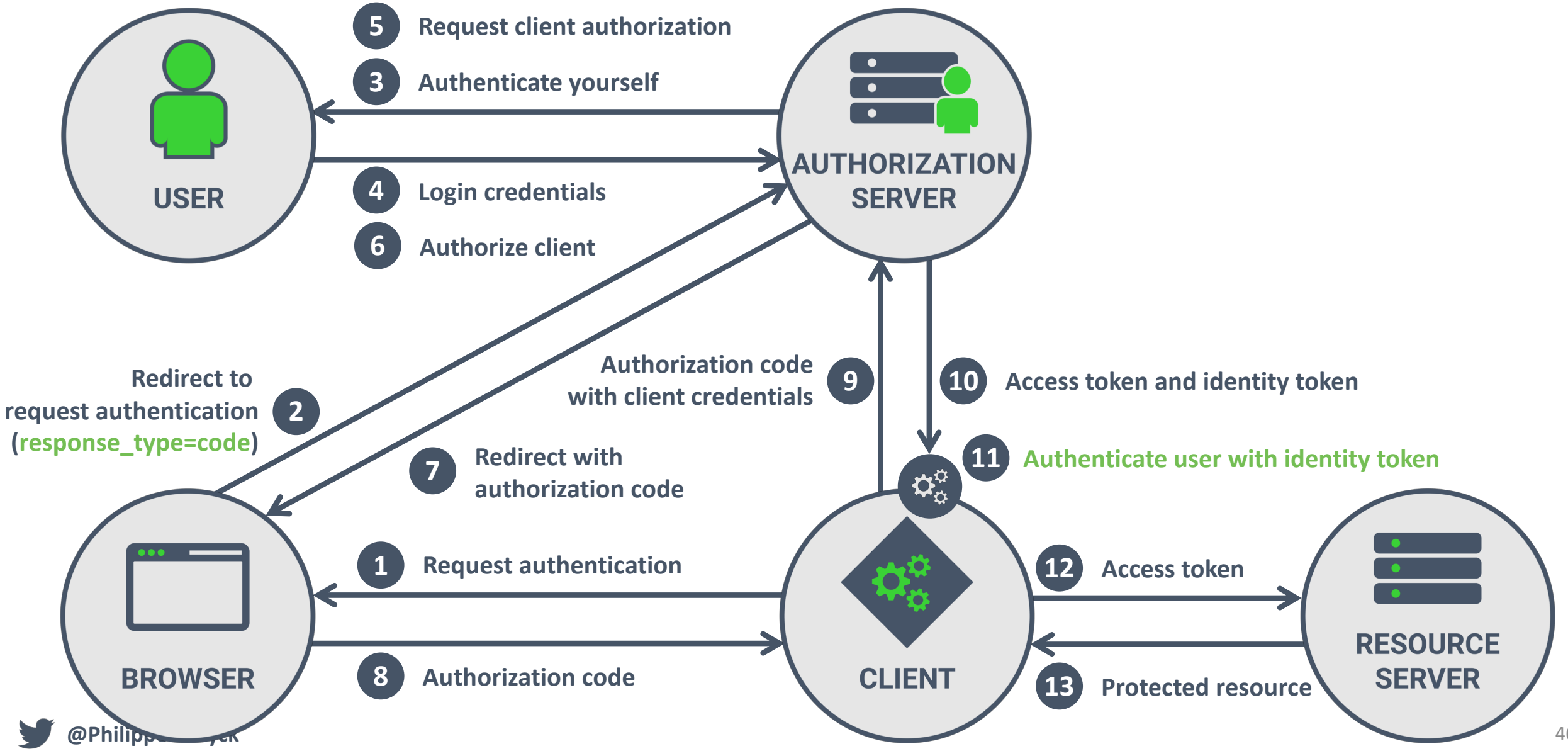
The OIDC Implicit Grant flow



Implicit grant

- Identity token is intended for the frontend application
- Allows establishing the user's identity in the frontend only

THE OIDC AUTHORIZATION CODE GRANT FLOW



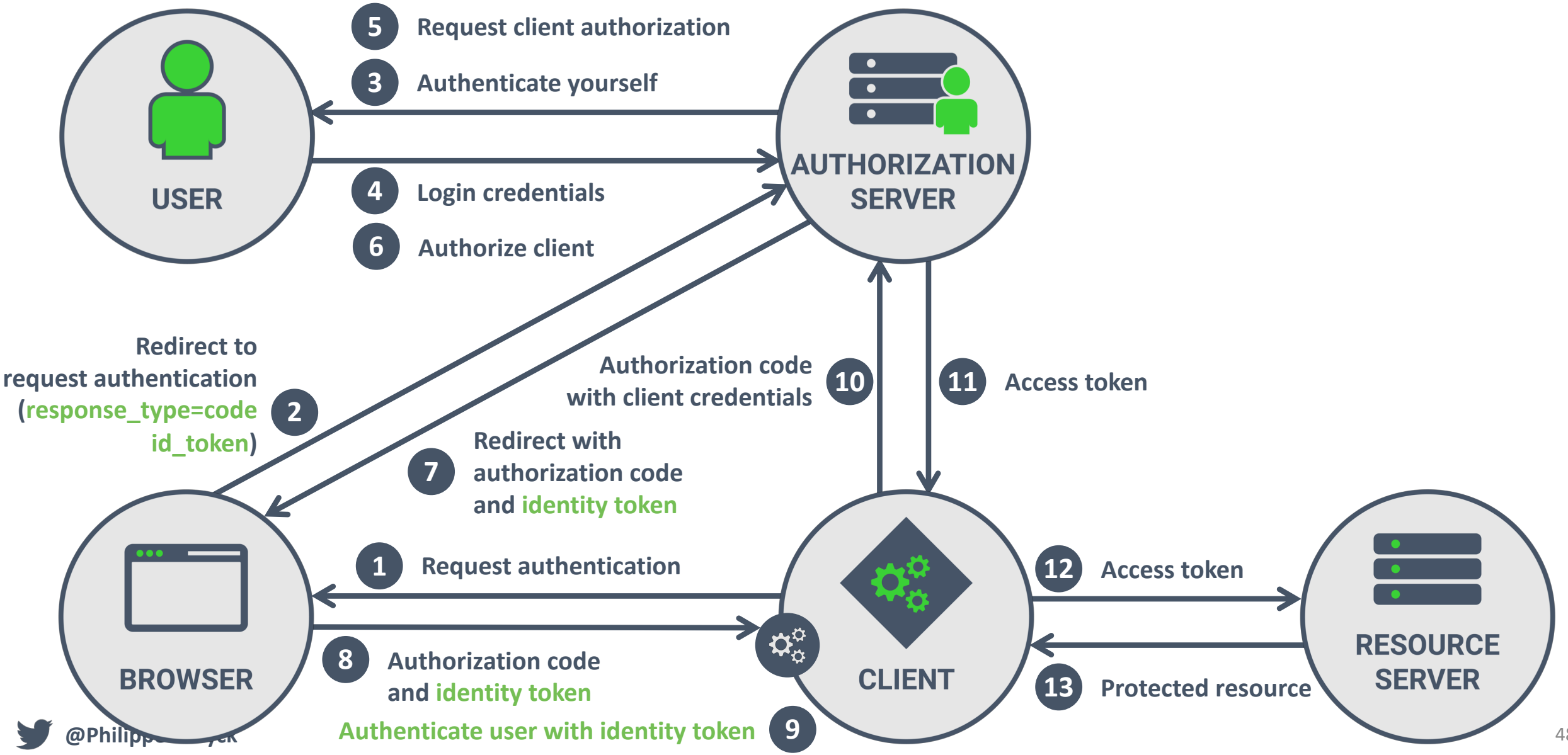
Implicit grant

- Identity token is intended for the frontend application
- Allows establishing the user's identity in the frontend only

Authorization code grant

- Identity token is intended for the backend application
- Allows connecting the identity of the user to an internal user concept

THE OIDC HYBRID FLOW



Implicit grant

- Identity token is intended for the frontend application
- Allows establishing the user's identity in the frontend only

Authorization code grant

- Identity token is intended for the backend application
- Allows connecting the identity of the user to an internal user concept

Hybrid

- Identity token is intended for the backend application
- Allows connecting the identity of the user to an internal user concept
- The backend must check if the audience of the token matches its client id

OAuth 2.0 offers delegation

OpenID Connect offers authentication

Pragmatic Web Security

Security training for developers

/in/PhilippeDeRyck

@PhilippeDeRyck

philippe@pragmaticwebsecurity.com