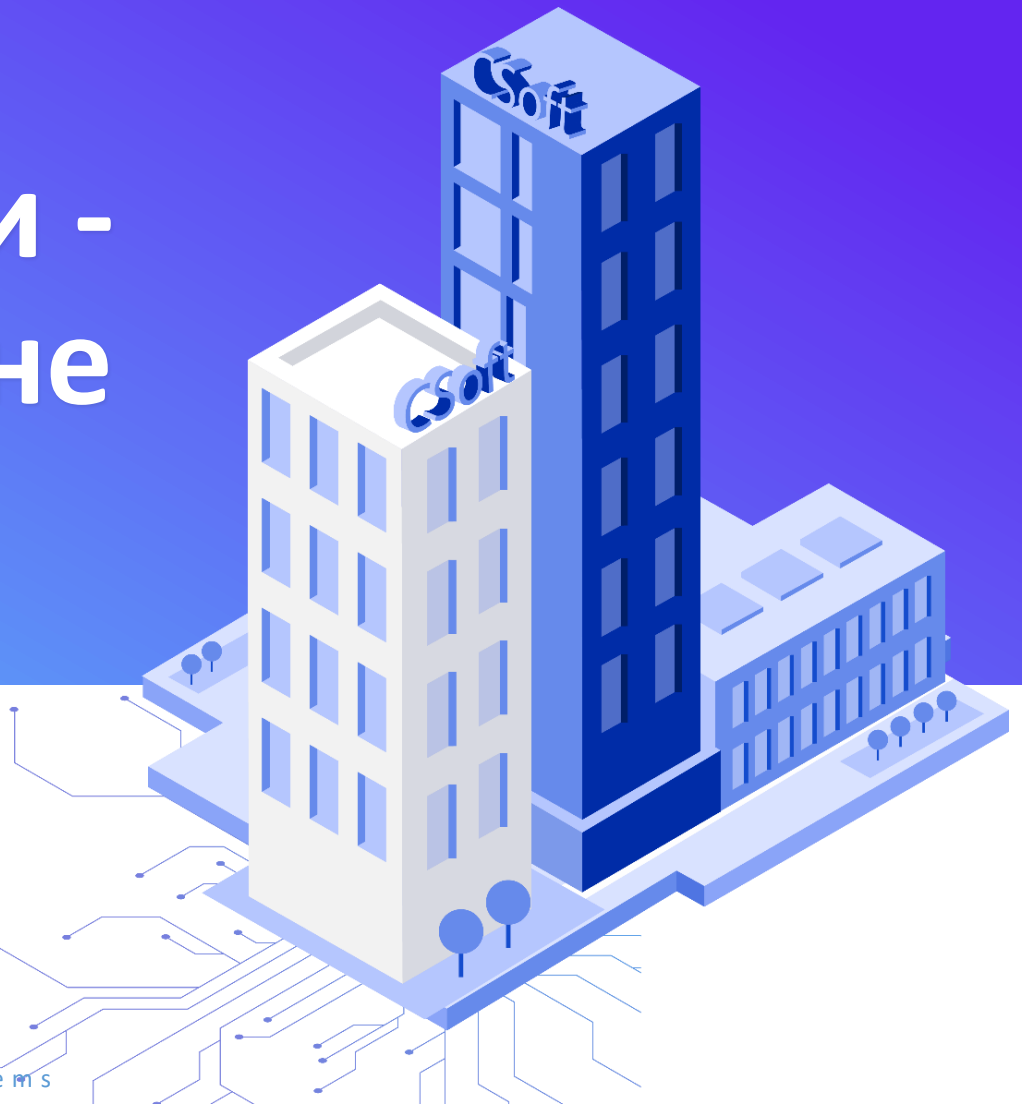
Запознаване с API програмни интерфейси - създаване, консумиране и сигурност



За нас

Веселин Стефанов

- Solution Architect в CSoft
- “I’m a greater believer in luck, and I find the harder I work the more I have of it.”
- Обичам да ходя, там където краката ме водят

Христиан Атанасов

- CTO в CSoft
- „Work to Learn and Impact. Don't work for money!“
- Обичам спорта и пътуванията

Кои сме Ние?

BrightOS Core Banking System

Front-end

Търговия с ЦК

Кредитни карти, Кредити, Депозити, Сметки

Плащания

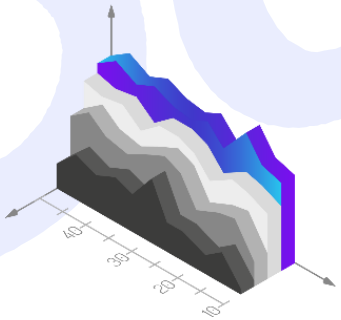
Базово счетоводство

Такси

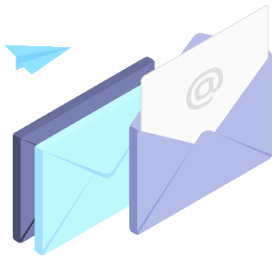
bMobile & bWeb

API Gateway

IFRS9



CSNotification



Postbank

INTERNATIONAL ASSET BANK

БНП ПАРИБА лични финанси

CAPITAL BANK

TBI Bank

ОБЩИНСКА БАНКА

БЪЛГАРСКА БАНКА ЗА РАЗВИТИЕ

НАЦИОНАЛЕН ГАРАНЦИОНЕН ФОНД

HCM

ACCESS FINANCE

За какво ще говорим?

Създаване на API

Консумиране на API

Сигурност

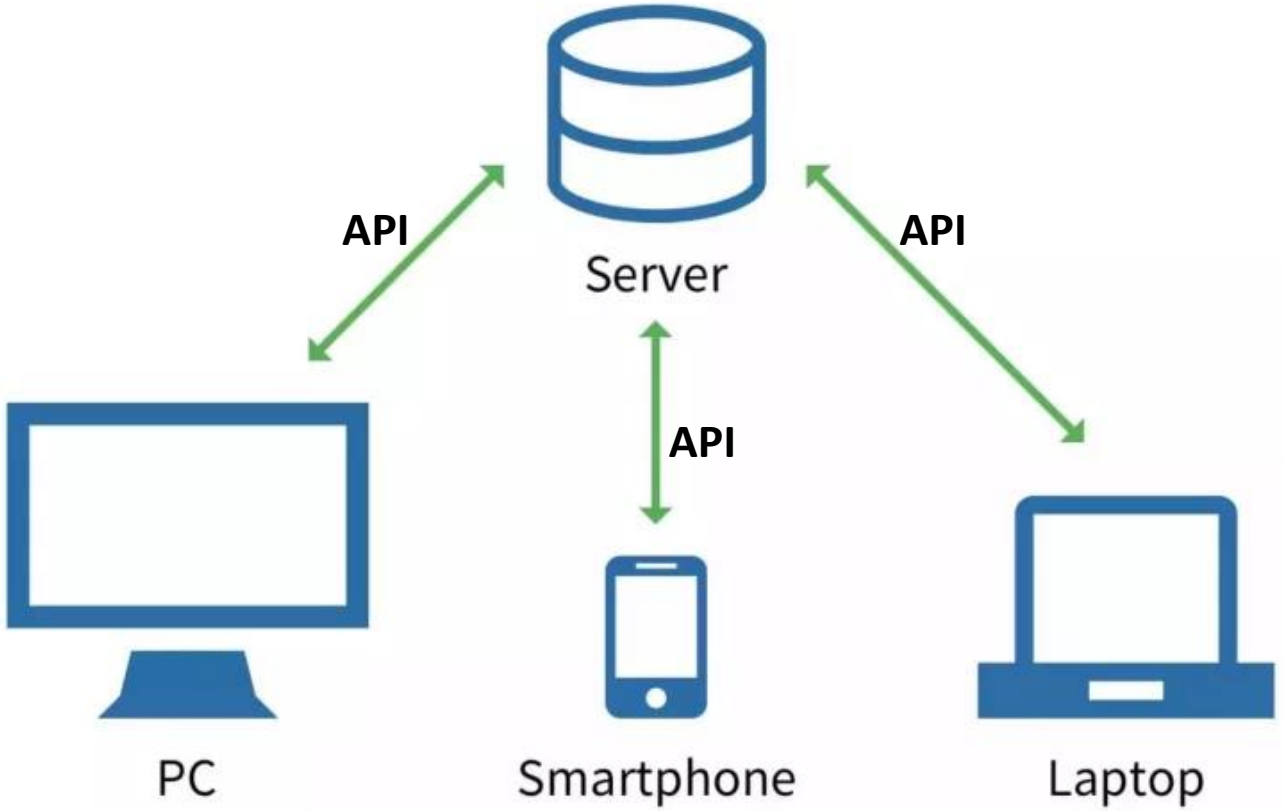
Създаване на API

Консумиране на API

Сигурност

Какво е API?

Създаване на API



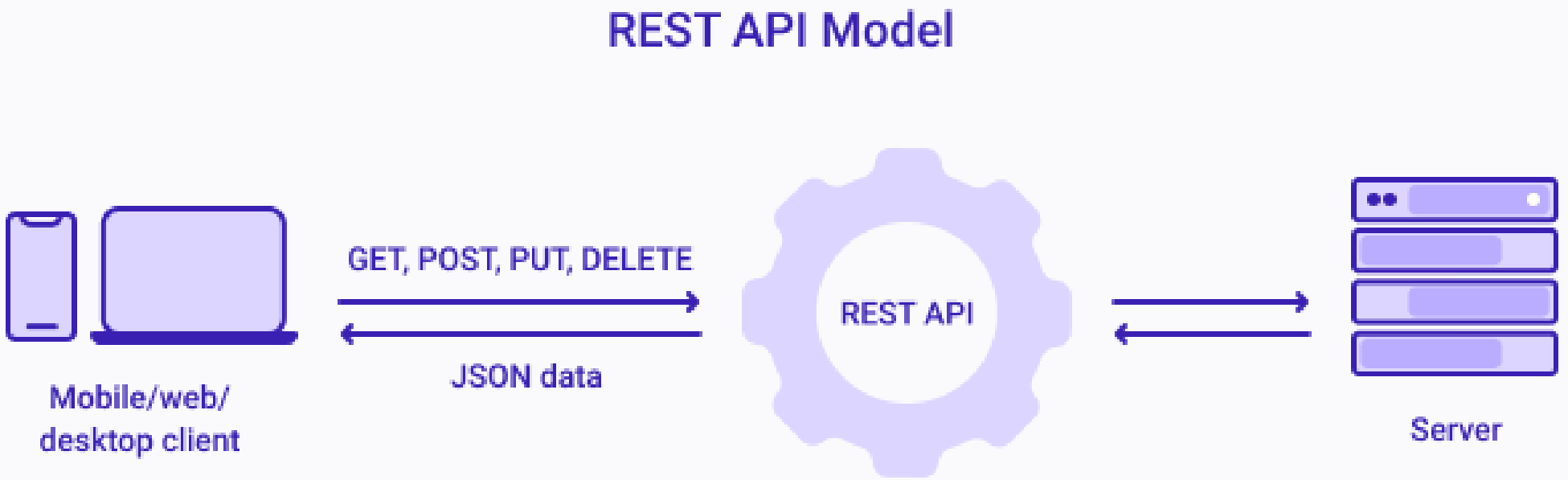
Протоколи

Създаване на API

- REST + JSON
- gRPC
- SOAP + XML (Legacy)

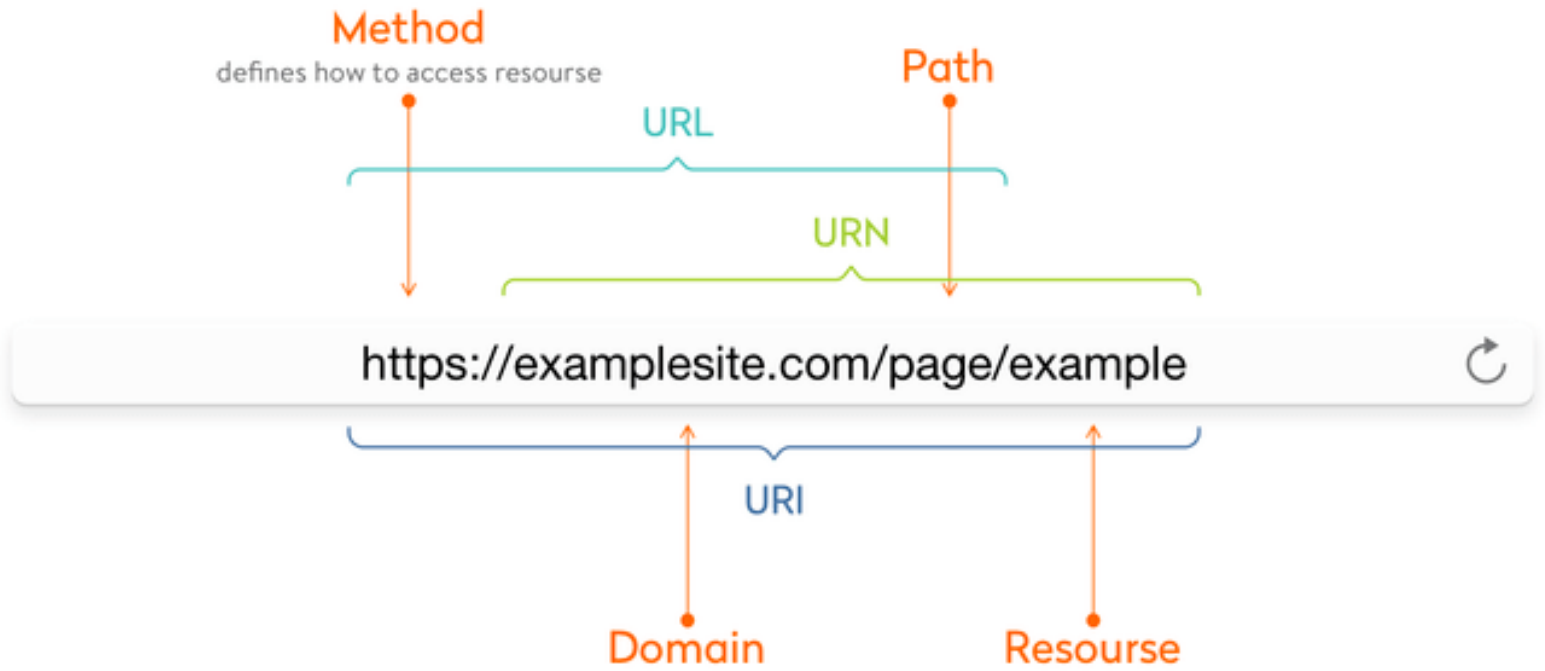
REST API Overview

Създаване на API



REST URI

Създаване на API



[Components of URI]

HTTP Methods

Създаване на API

- **GET**
- **POST**
- PUT
- DELETE

HTTP Methods

Създаване на API

Task	Method	Path
Create a new task	POST	/tasks
Delete an existing task	DELETE	/tasks/{id}
Get a specific task	GET	/tasks/{id}
Search for tasks	GET	/tasks
Update an existing task	PUT	/tasks/{id}

HTTP Status Codes

Създаване на API

HTTP Status Codes

Създаване на API

HTTP Status Codes

Създаване на API

HTTP Status Codes

Създаване на API

HTTP Status Codes

Създаване на API

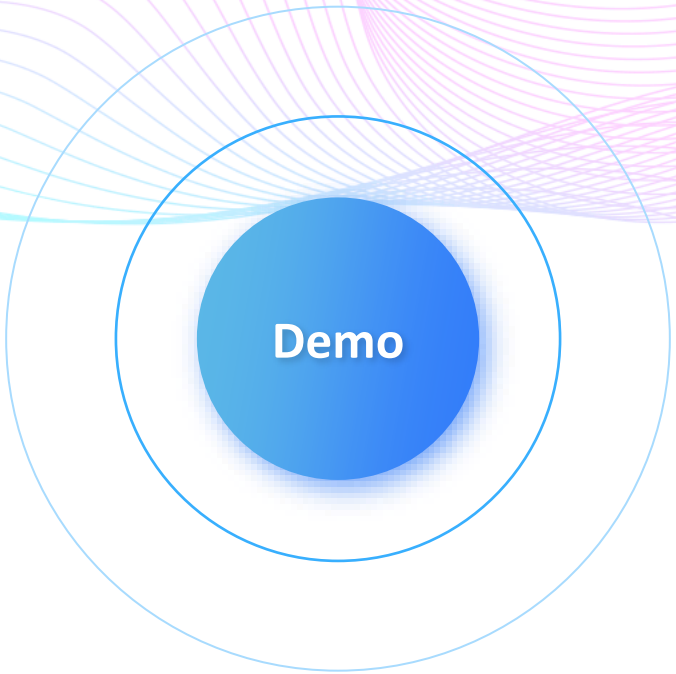
Платформи

Създаване на API

- **Microsoft IIS, Kestrel | .NET Core Web API**
- **NodeJS | JavaScript**
- **Python**
- **Apache | PHP**
- **Друго**

API Server-side

.NET WebAPI Sample



Създаване на API

Консумиране на API

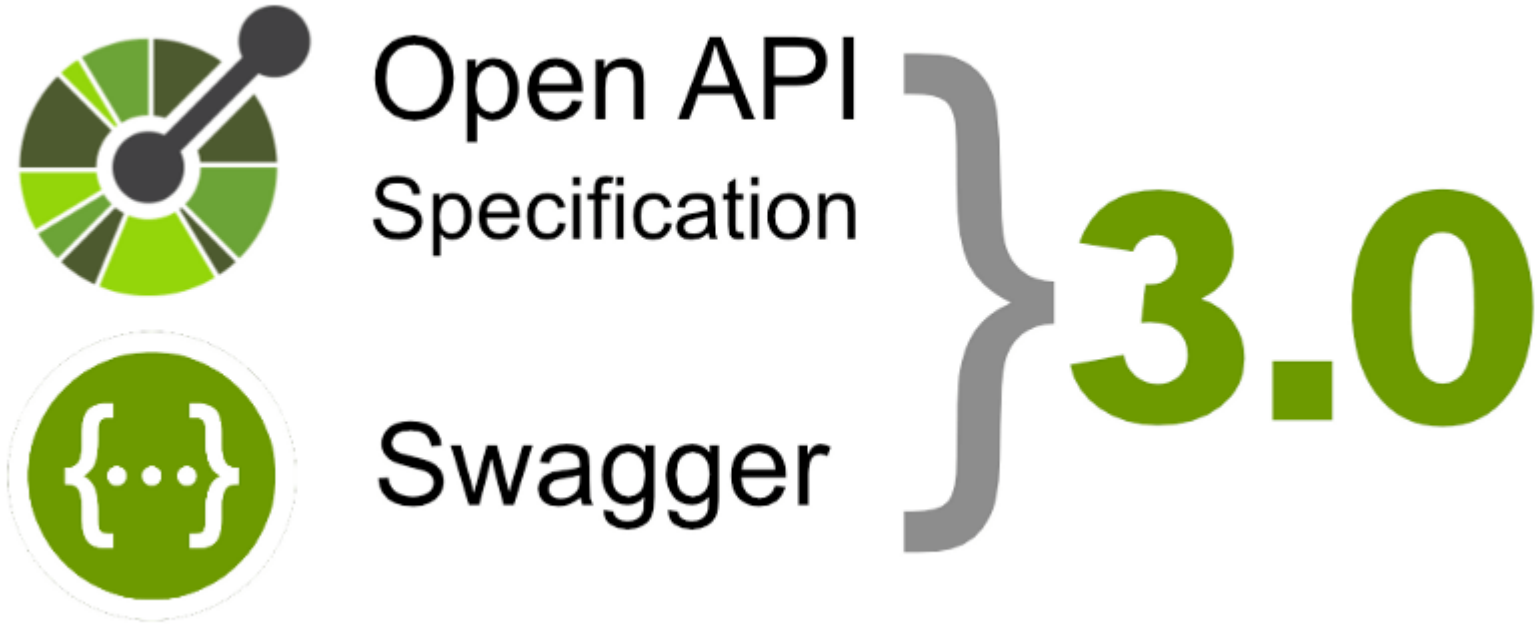
Сигурност

OpenAPI.

OpenAPI Specification (OAS)

OpenAPI

Консумиране на API



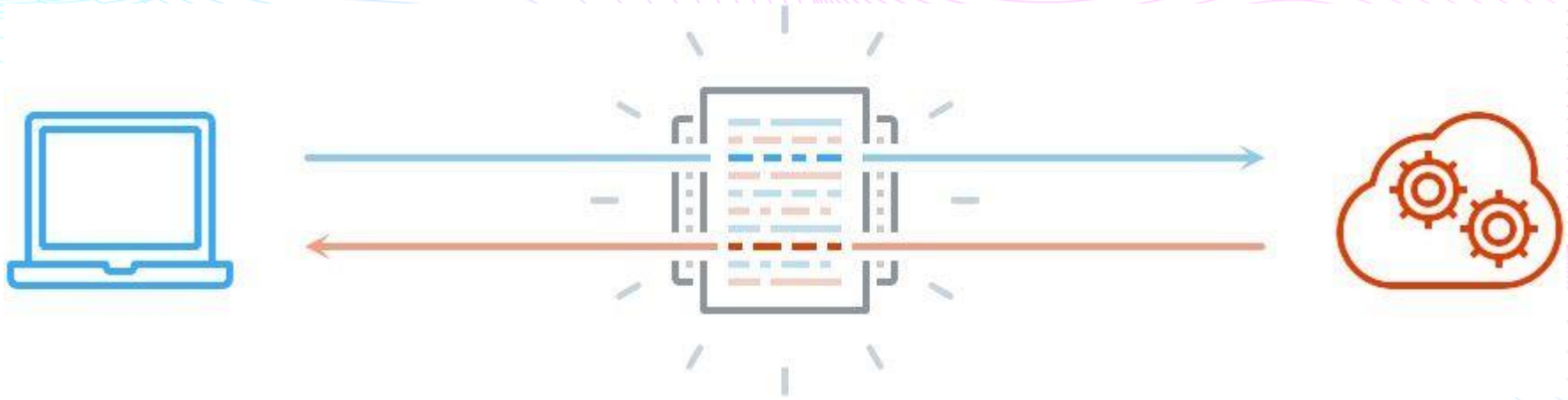
Какво е OpenAPI?

Консумиране на API

"The OpenAPI Specification (OAS) defines a standard, programming language-agnostic **interface description for HTTP APIs**, which **allows both humans and computers to discover and understand** the capabilities of a service without requiring access to source code, additional documentation, or inspection of network traffic."

OpenAPI

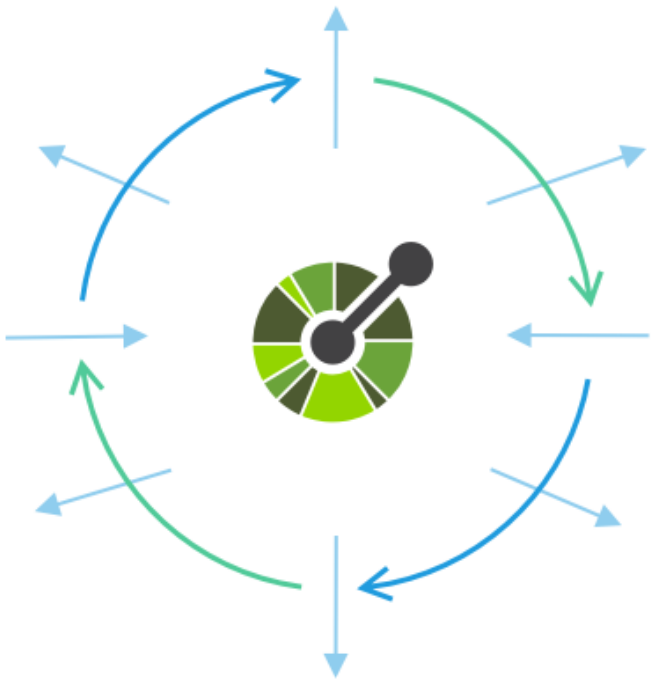
Консумиране на API



https://editor.swagger.io/ ❐

OpenAPI

Консумиране на API



IMPLEMENTATION

Generated server code/artifacts

TESTING

Functional, security, load, compliance, etc.

VIRTUALIZATION

Functional/Runtime simulations

DOCUMENTATION

Developer portals, code samples, user guides, etc

DEPLOYMENT/RUNTIME

Security, usage policies, monitoring, caching, etc

CLIENTS

Generated client libraries

DESIGN

Object reuse, linking, callbacks, etc

MOCKING

Prototyping

Кой използва OpenAPI?

CSoft

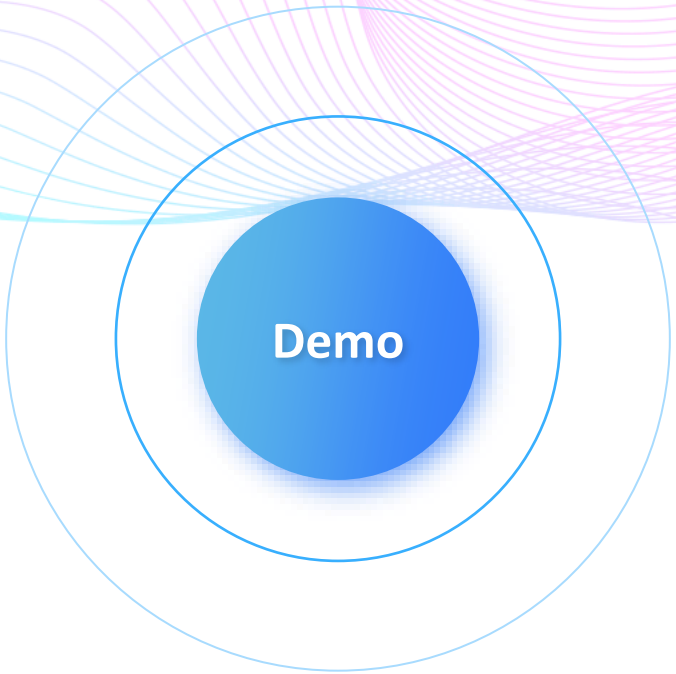
Microsoft

Google

Atlassian

OpenAPI

Console App Sample



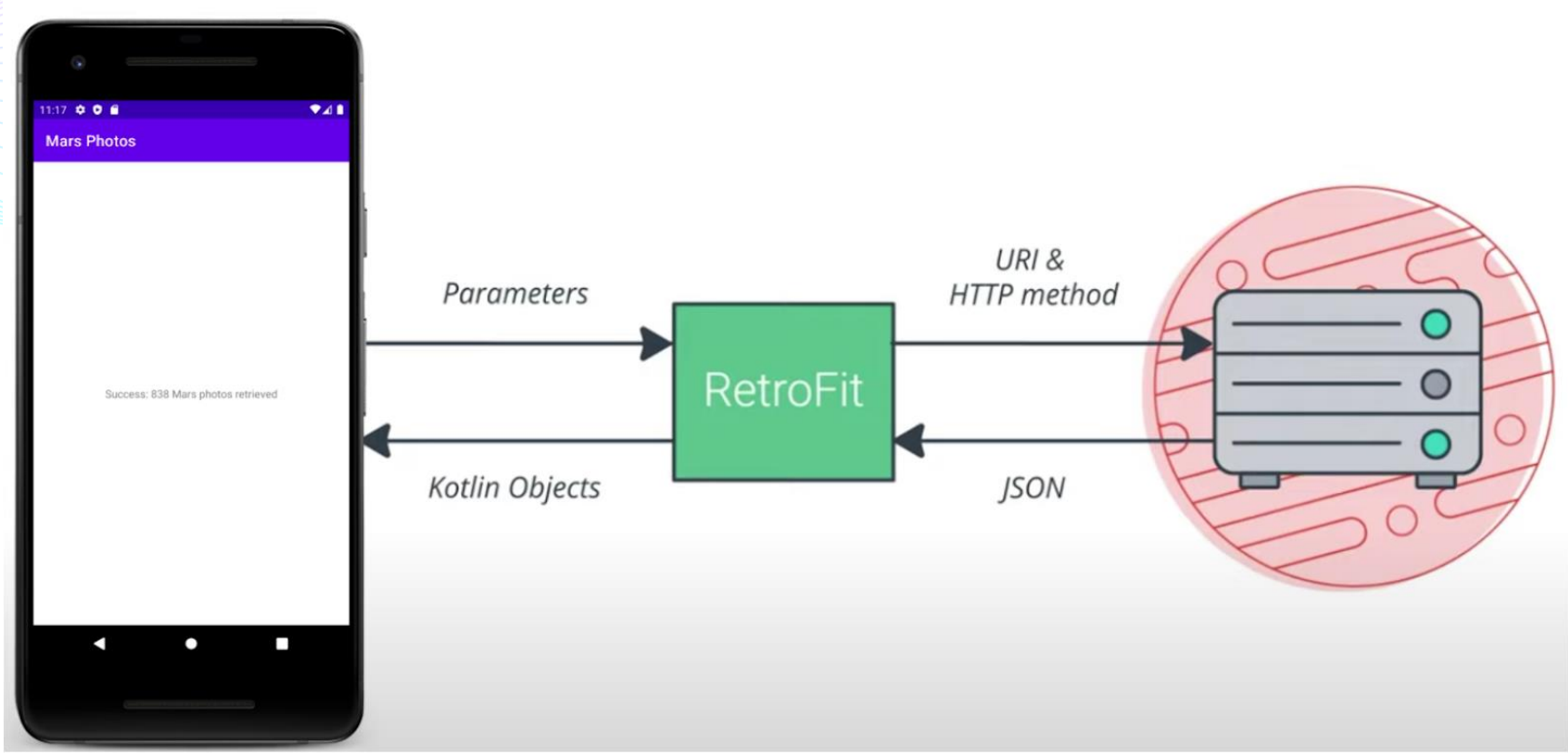
Android and Retrofit.

Calling APIs from Android App

Retrofit2

Retrofit2

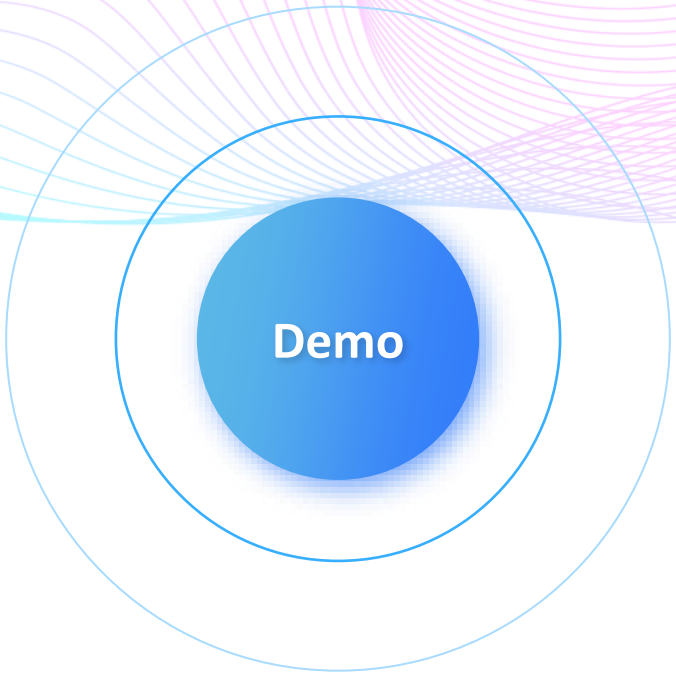
- **Type-safe** HTTP Client
- **Annotations** to describe the HTTP Request
- **Plain Objects** <> JSON

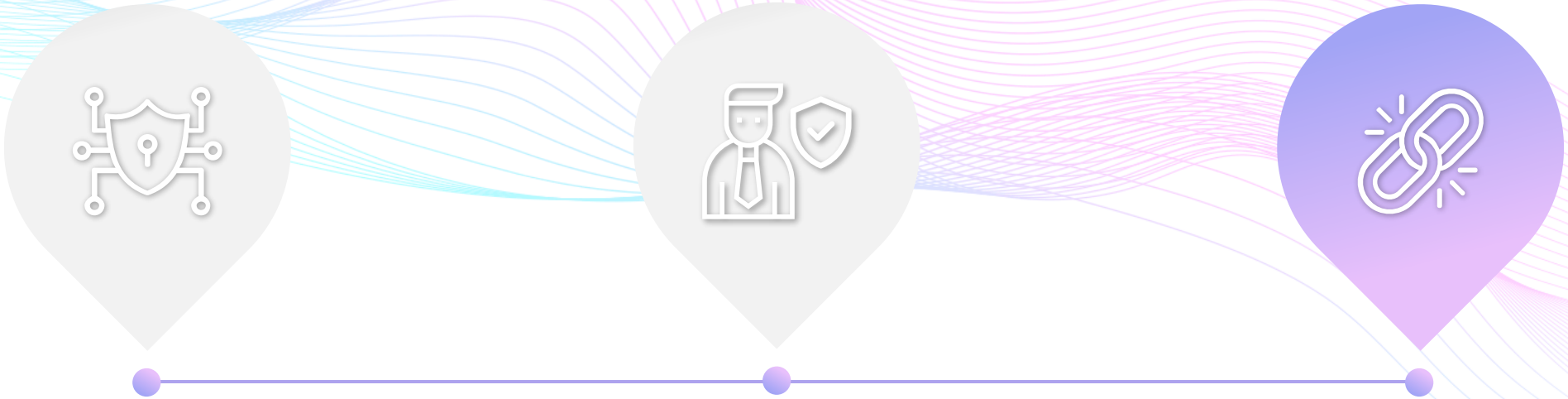


https://github.com/square/retrofit

Calling APIs from Android App

Retrofit2 Sample



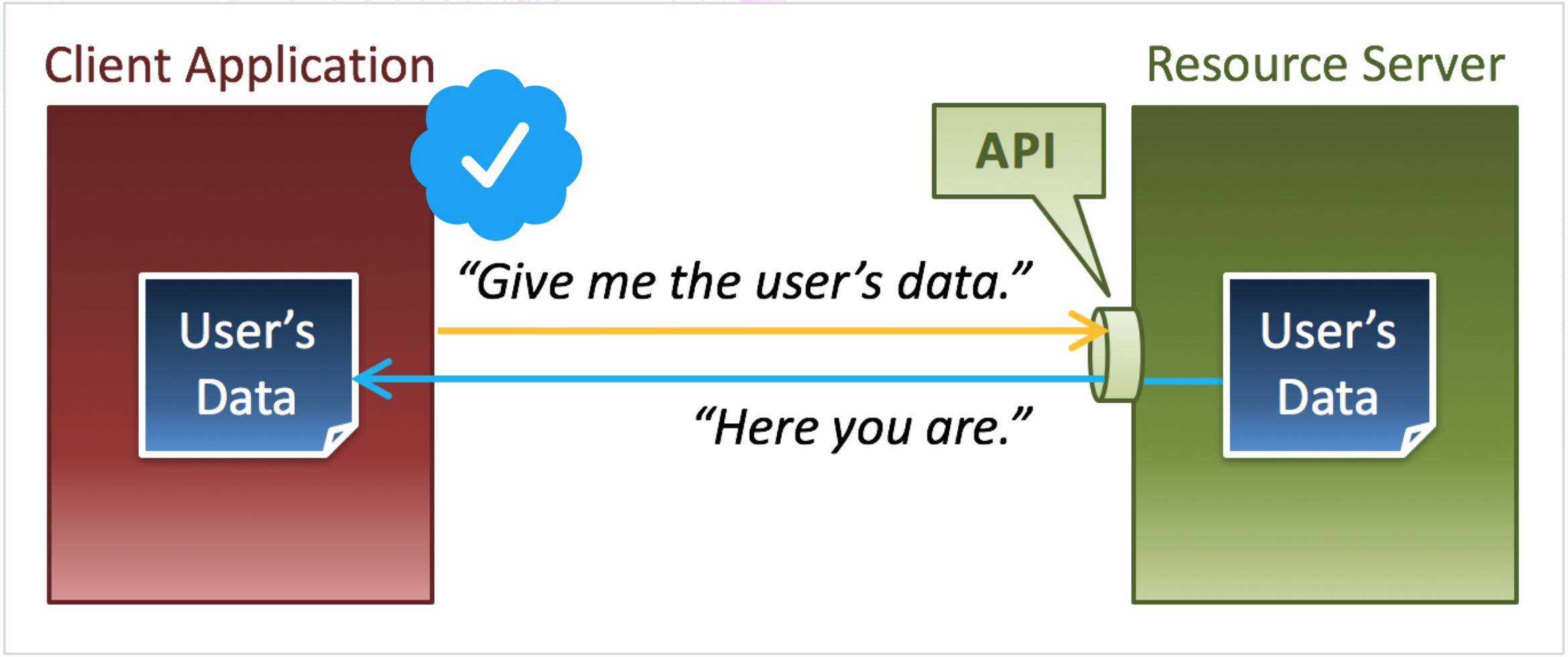


Създаване на API

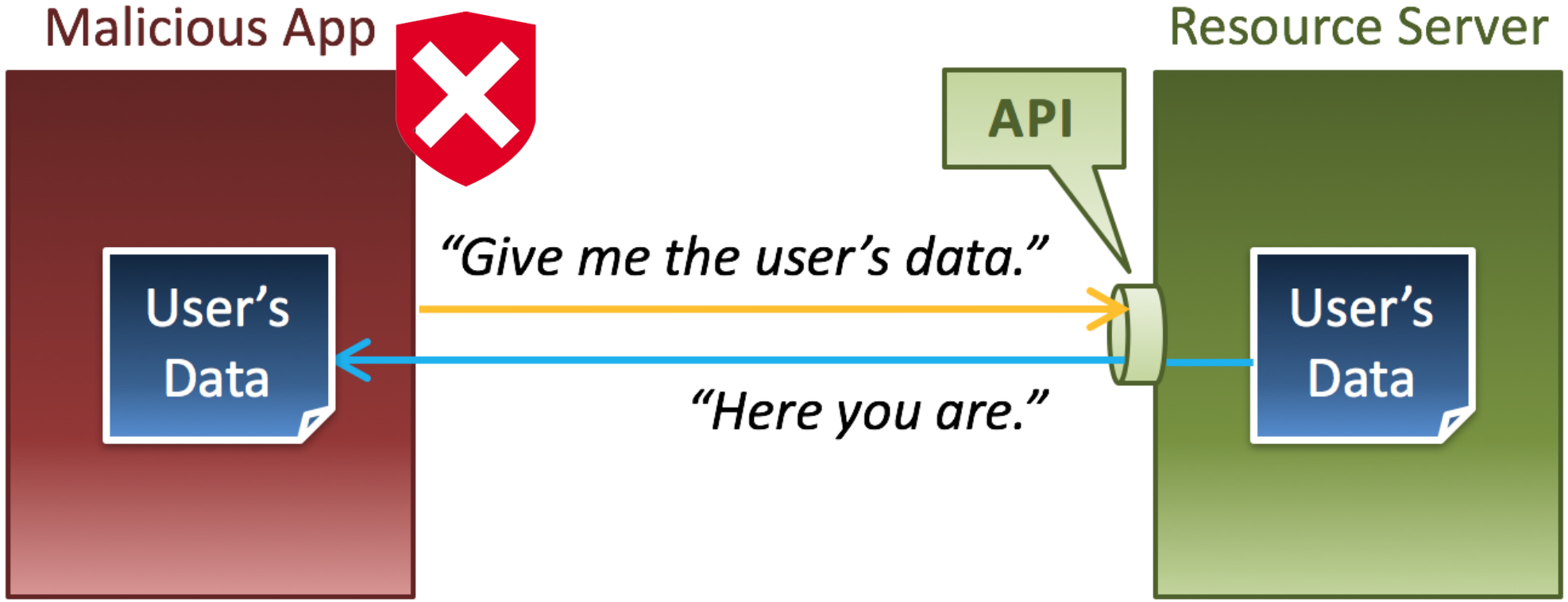
Консумиране на API

Сигурност

Автентикация и защо ни трябва

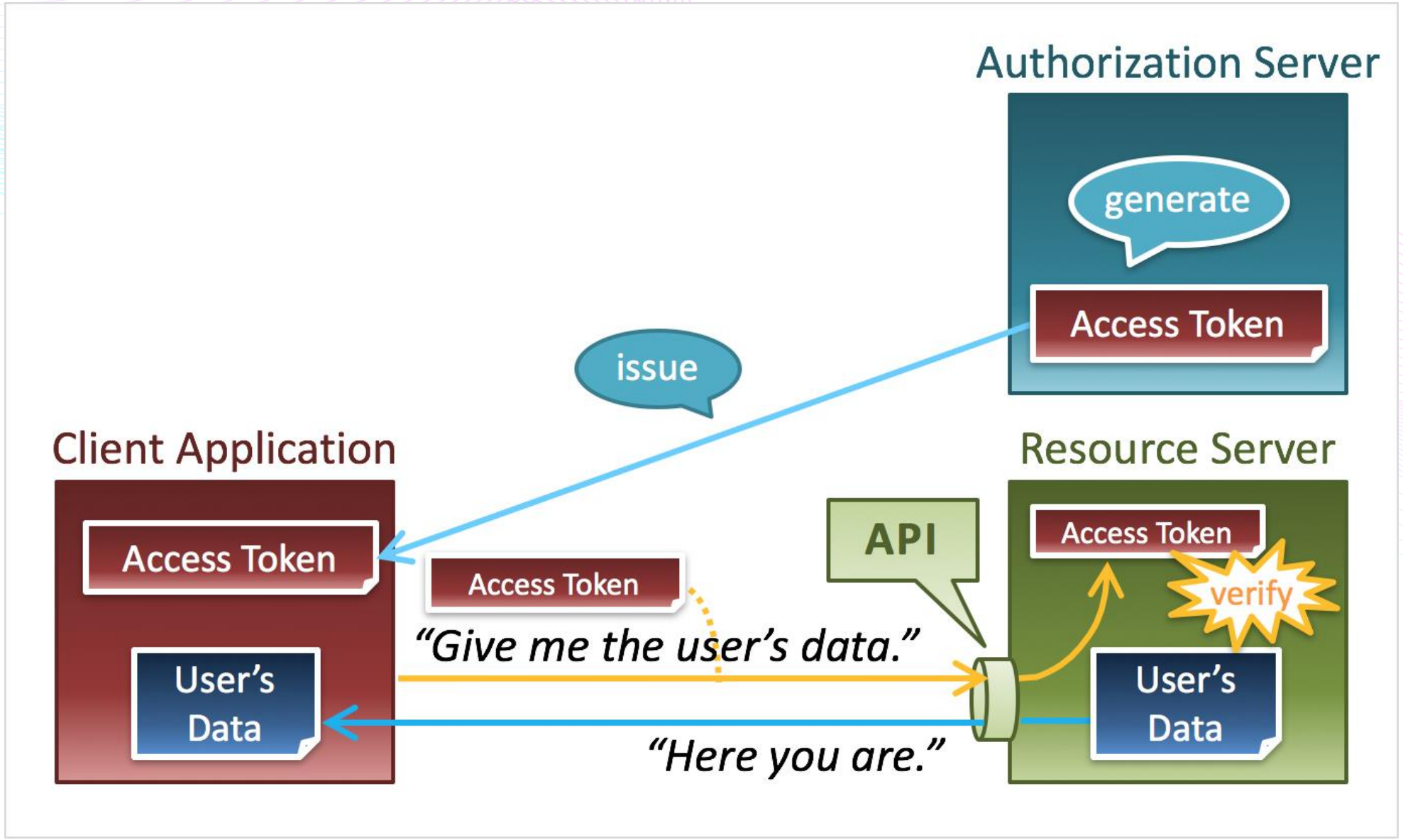


А ако друг иска да достъпи User’s Data?



Even a malicious application can get the user’s data.

Access Token

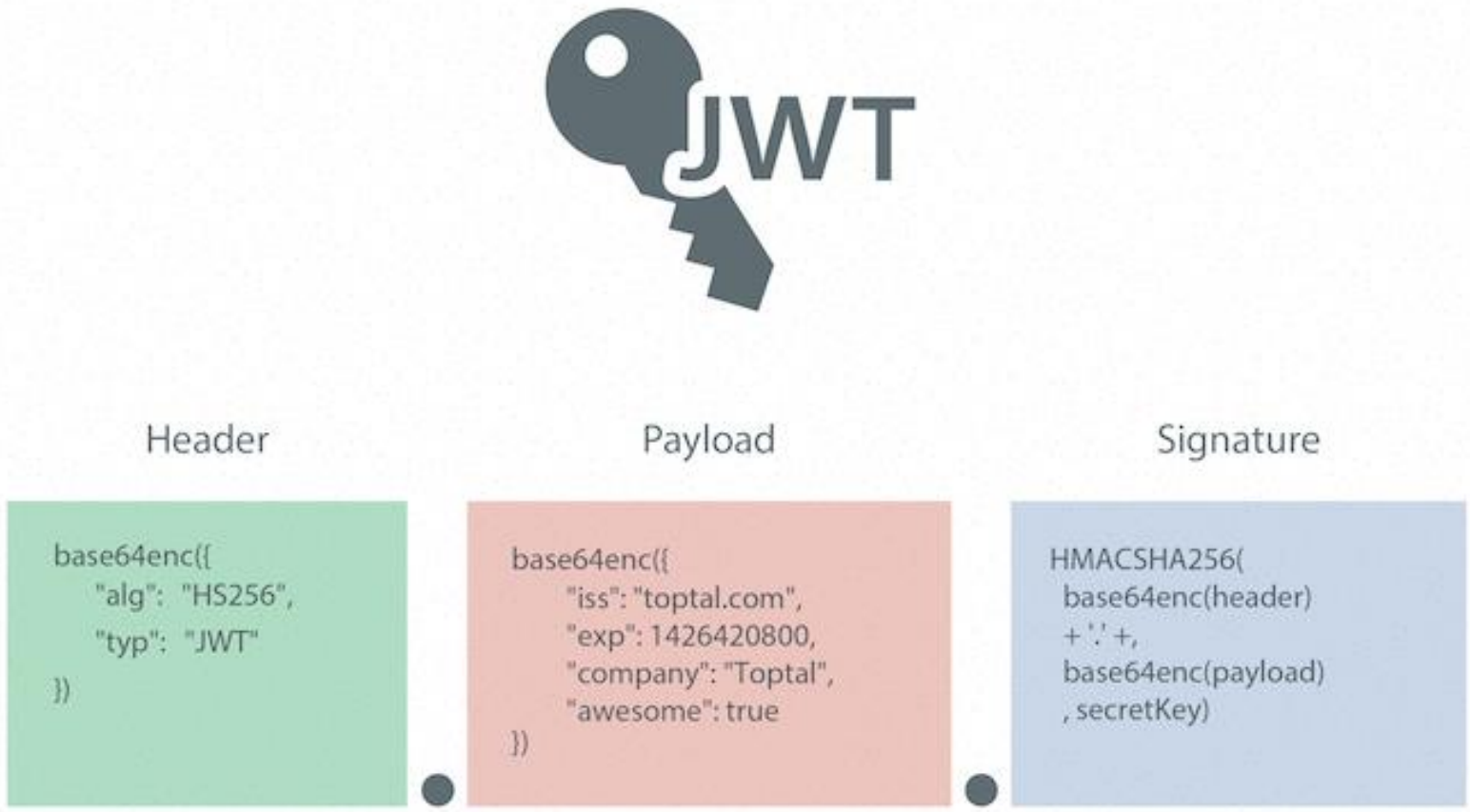


JWT Access Token

JWT =
JSON Web Token

- Header
- Payload and Claims
- Signature

https://jwt.io/



API Security Top Tips

API Security Top Risks

Broken Object Level Authorization

Имам ли право да достъпя този обект

Excessive Data Exposure

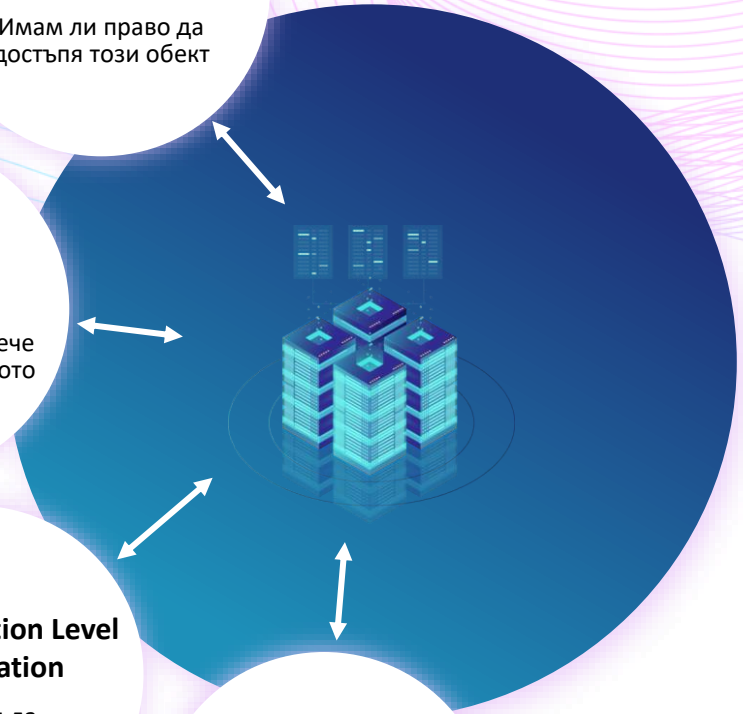
Expose на много повече данни от необходимото

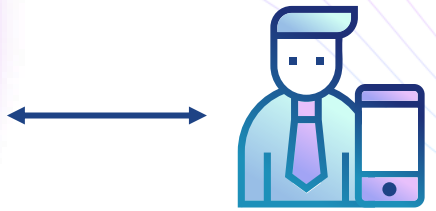
Broken Function Level Authorization

Мога ли да достъпвам Admin панел, ако съм Client на ClientApp

Broken Authentication

Създаване на незащитени APIs, считани за internal





ClientApp.

Broken Object Level Authorization

https://api.com/payments/8375

*Транзакция на **Христиан Атанасов***

https://api.com/payments/8376

Транзакция на Иван Петров

Broken Object Level Authorization

How to Prevent

Как да се защитим?

- User Access Checks за право на достъп
- Use Random non-guessable IDs (UUIDs)

https://api.com/payments/69e43ae4-d051-11ec

*Транзакция на **Христиан Атанасов***

Excessive Data Exposure

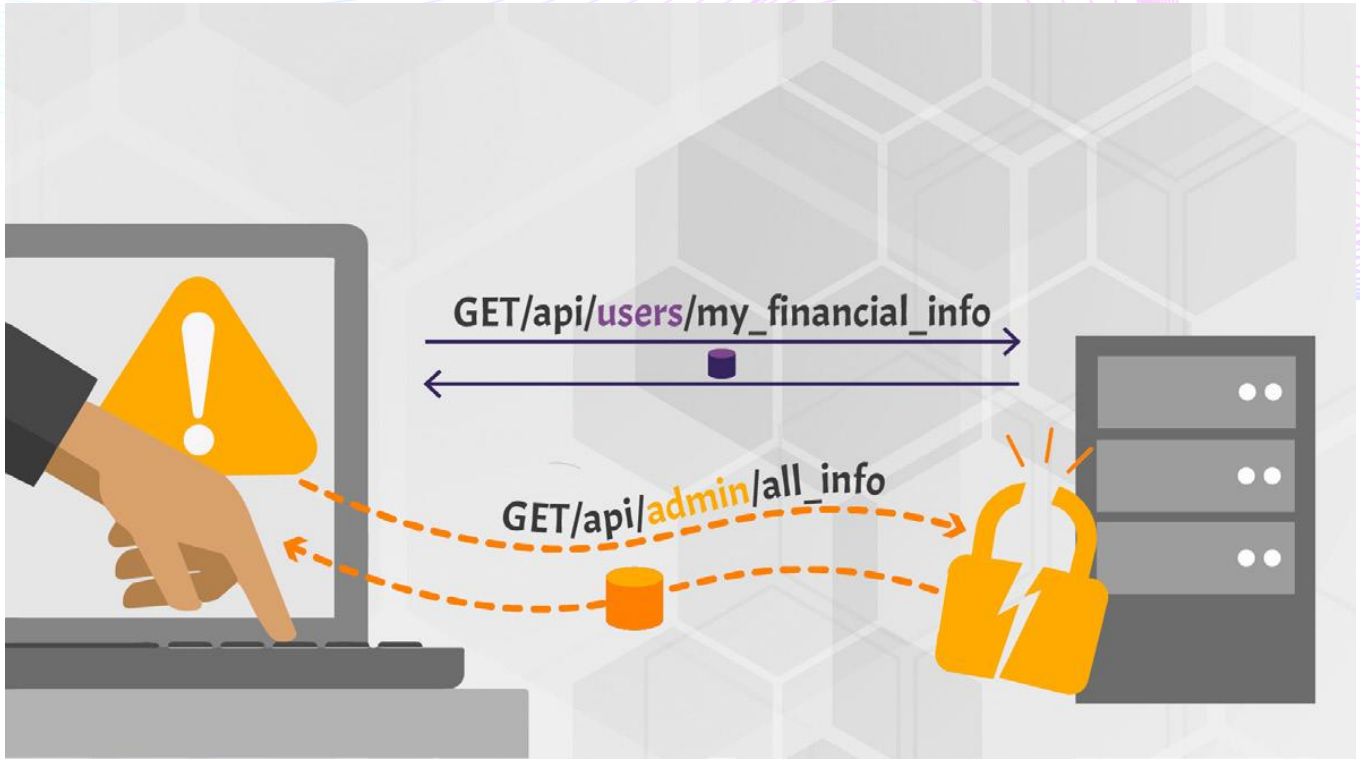
Excessive Data Exposure

How to Prevent

Как да се защитим?

- Никога не разчитайте на клиента да филтрира данни
- **Разглеждайте данните, които ще се представят и мислете**
- Имайте ясна представа какво е **„лични данни“** и не го споделяйте
- Не съкращавайте имена на променливи, за да може Audit Review да спаси

Broken Function Level Authorization



Use Cases.

- Expose на Admin функции за потребители без съответните права
- Липса на role-based privileges подход при предоставяне на Admin features

Broken Function Level Authorization

How to Prevent

Как да се защитим?

- Не разчитайте на ClientApp да защити вашия Admin access
- **Deny by Default – най-добре с базови класове**
- Имплементирайте role-base достъп до feature-и. Например ClientApp | CustomerSupport | Reporting | Administrator
- Penetration Tests – добра практика е след развой новите APIs да бъдат тествани

Broken Authentication

Use Cases.

- Незащитени APIs, считани за internal
- **Запазване на пароли в базите данни в plain text (или криптирани)**
- Липсващи изисквания за силни пароли
- Липса на механизми за force на подмяна на пароли, API Keys
- Липса на 2FA

Broken Function Level Authorization

How to Prevent

Как да се защитим?

- Не позволявайте достъп до вашето API без автентикация, дори и на internal systems
- **Hash your Passwords (+ Salt!)**
  - **както at-rest в Database**
  - **така и при transfer ClientApp <> Server**
- Създайте минимални изисквания за сложност на паролите, както и политики за подмяната им

Възможности при нас

Стажантската програма

Защо е за вас?

- ✓ Създавате ваше, завършено приложение
- ✓ Използвате технологии на практика
- ✓ Получавате обратна връзка от опитни ментори
- ✓ Учите се да работите по задачи със срок
- ✓ Решавате дали сме вашето място за развитие
- ✓ Започвате постоянна работа

Предстоящ стаж през юли 2022

Вашите въпроси:

CSoft

Въпроси?

Imagine. Reinvent. Accelerate.

Bravely climbing the steps of success