Rakamin

Secure Coding

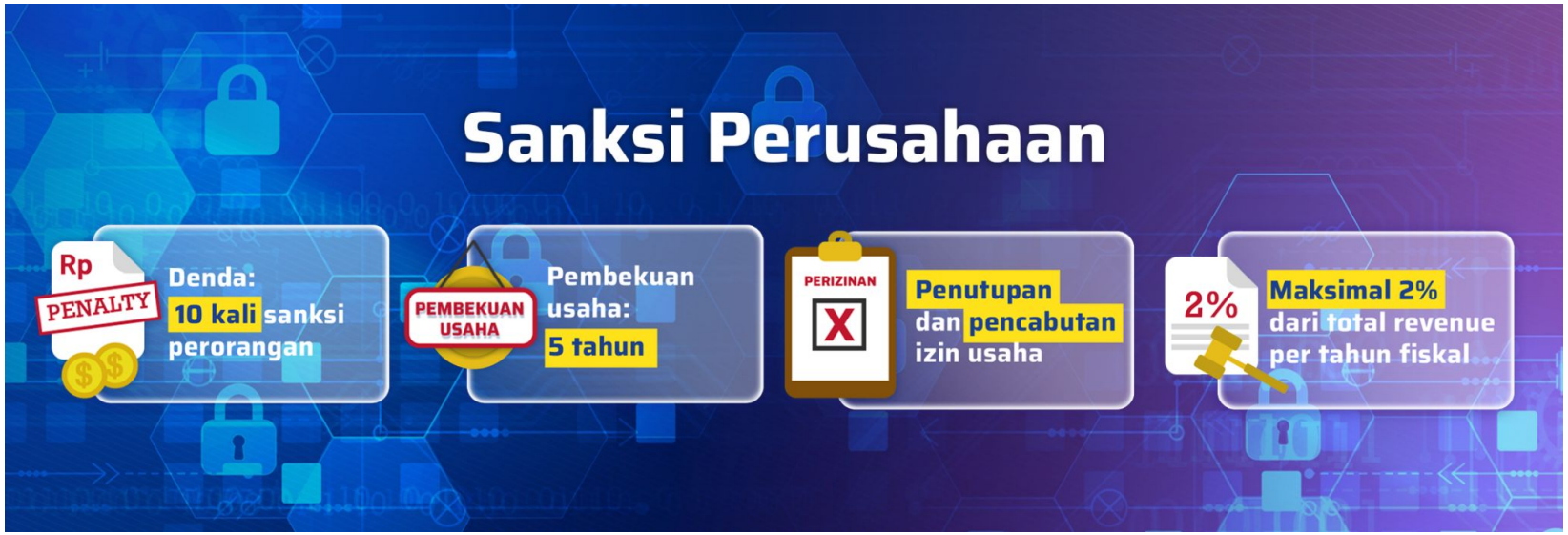
Authentication & Authorization

Autentikasi & Otorisasi – Kunci Keamanan API di Indonesia

Transformasi digital Indonesia (e-commerce, fintech, layanan publik) bergantung pada API. Namun, ancaman mengintai:

- **2 juta data nasabah bocor** karena autentikasi lemah (2022).
- **Pelanggaran UU PDP** berisiko denda hingga 2% pendapatan perusahaan.

Autentikasi memastikan "siapa yang boleh masuk", sementara **otorisasi** mengatur "apa yang boleh dilakukan". Tanpa keduanya, API seperti rumah tanpa kunci – siapa pun bisa masuk dan mengambil segalanya.



1. Authentication (Autentikasi)

Proses memverifikasi identitas pengguna/sistem yang mengakses API (misal: username-password, token, atau biometrik).

Contoh Kasus di Indonesia:

- Pengguna login ke aplikasi e-commerce (contoh: Tokopedia) dengan OTP (One-Time Password) via SMS.
- Aplikasi pembayaran digital (Gojek/DANA) menggunakan PIN/biometrik untuk autentikasi transaksi.

Vulnerabilitas Umum (OWASP API Top 10):

- **Broken Authentication** (No. 2):
  - Token JWT yang tidak divalidasi dengan benar.
  - API keys yang terpapar di kode sumber GitHub.
  - Serangan brute force pada endpoint login.

1. Authentication (Autentikasi)

Contoh Serangan di Indonesia:

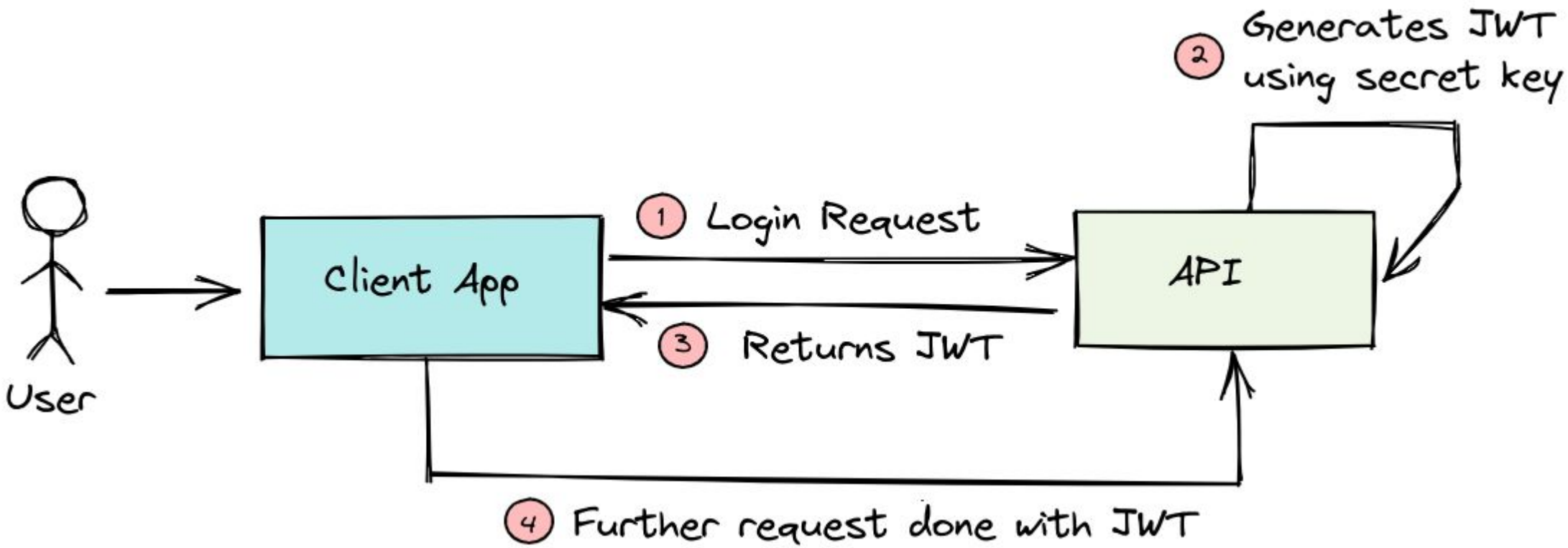
- Kasus pembobolan akun pengguna *e-wallet* karena OTP lemah atau kebocoran API key.

Best Practices:

- Gunakan **OAuth 2.0** atau **OpenID Connect** untuk autentikasi terstandar.
- Implementasi **Multi-Factor Authentication (MFA)** (contoh: OTP + biometrik).
- **Rate limiting** pada endpoint autentikasi untuk cegah brute force.

Rakamin

2. Authentication (Code Flow)



2. Authorization (Otorisasi)

Proses menentukan hak akses pengguna/sistem yang sudah terautentikasi (misal: izin baca/tulis data).

Contoh Kasus di Indonesia:

- Nasabah bank hanya bisa melihat data rekening sendiri (tidak bisa akses rekening orang lain).
- Driver Gojek hanya bisa melihat pesanan di wilayah operasionalnya.

Vulnerabilitas Umum (OWASP API Top 10):

- **Broken Object Level Authorization (BOLA)** (No. 1):
  - Manipulasi parameter ID (contoh: /users/123 diubah ke /users/456).
- **Broken Function Level Authorization** (No. 5):
  - Pengguna biasa mengakses endpoint admin (contoh: DELETE /api/admin/users).

Rakamin

2. Authorization (Otorisasi)

Contoh Serangan di Indonesia:

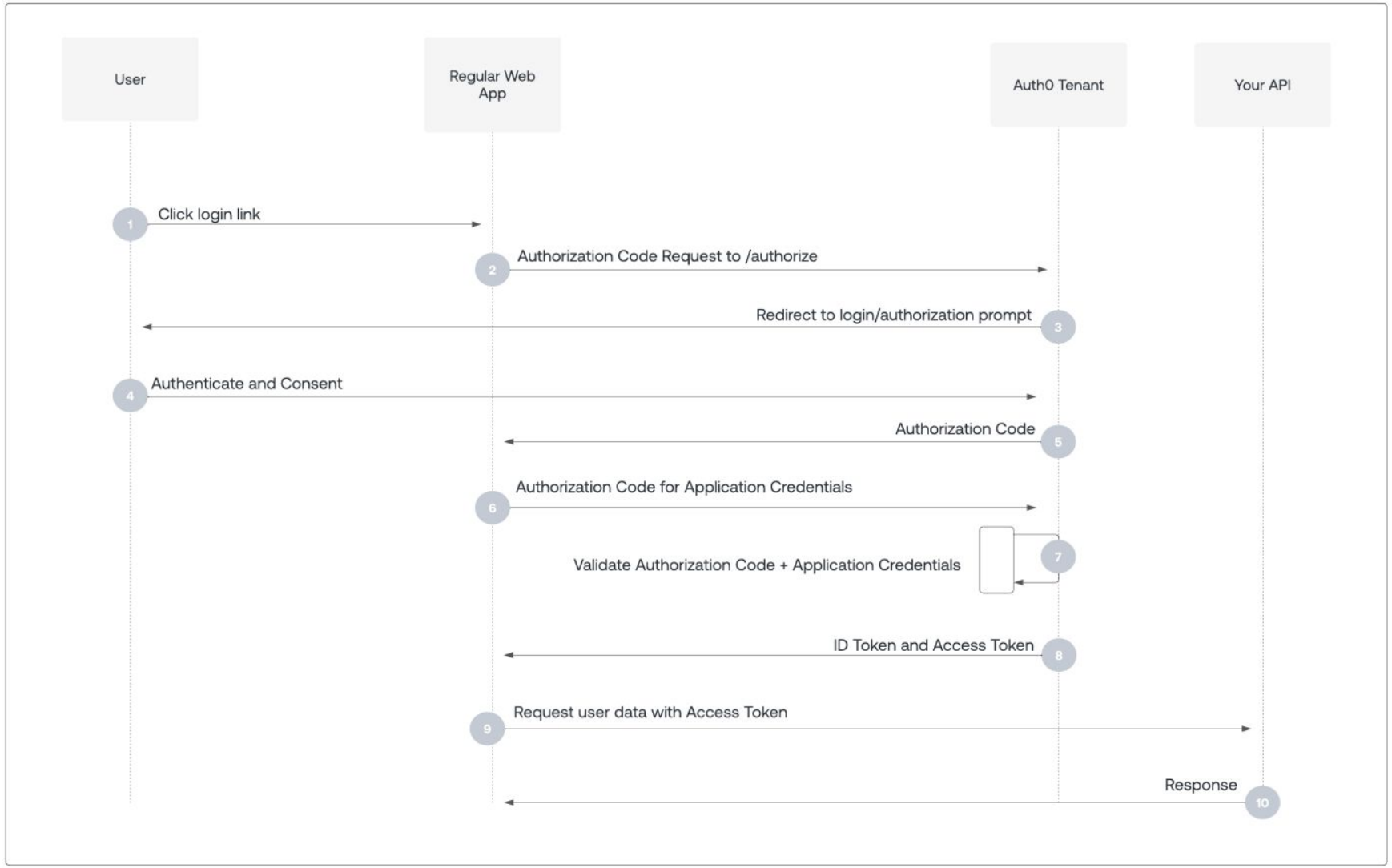
- Kebocoran data pasien rumah sakit karena validasi *role* tidak ketat (2023).
- Penyalahgunaan API *admin* startup fintech oleh insider.

Best Practices:

- Terapkan **Role-Based Access Control (RBAC)** atau **Attribute-Based Access Control (ABAC)**.
- Validasi izin akses di **setiap lapisan** (backend, database, cache).
- Gunakan UUID alih-alih ID berurutan untuk mitigasi BOLA.

Rakamin

2. Authorization (Code Flow)



Rakamin

Perbedaan Utama

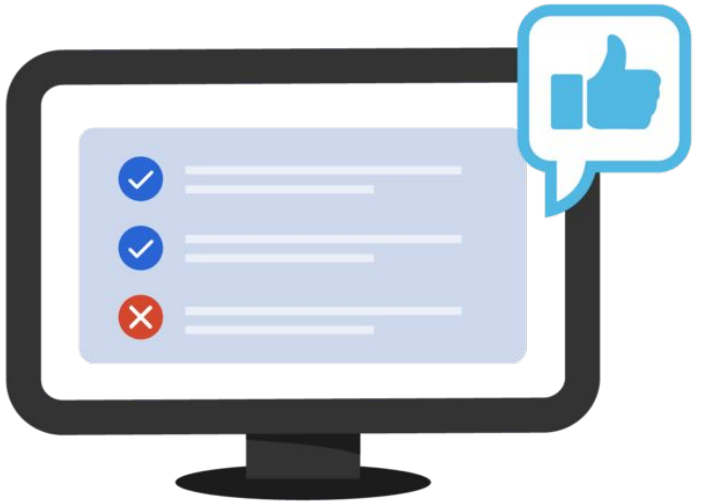
Aspek	Authentication	Authorization
Tujuan	Verifikasi identitas pengguna/sistem.	Menentukan hak akses pengguna.
Contoh Tools	OAuth 2.0, JWT, SAML.	RBAC, ABAC, Policy Engine (Open Policy Agent).
Contoh Kerentanan	Token yang bocor, serangan credential stuffing.	BOLA, akses fungsi admin tanpa izin.

Rakamin

Authentication

Confirms users
are who they say they are.

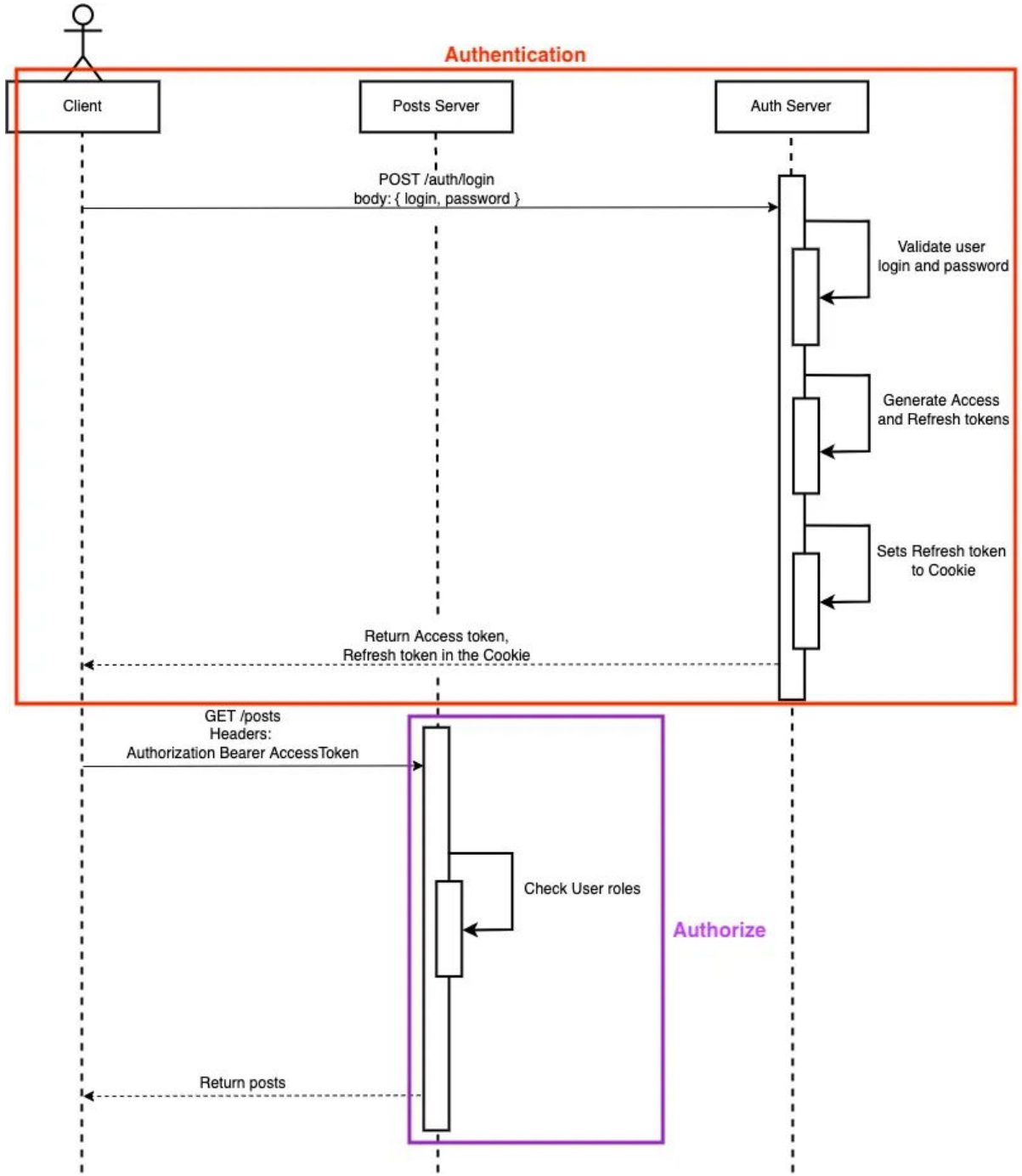
Authorization



Gives users permission
to access a resource.

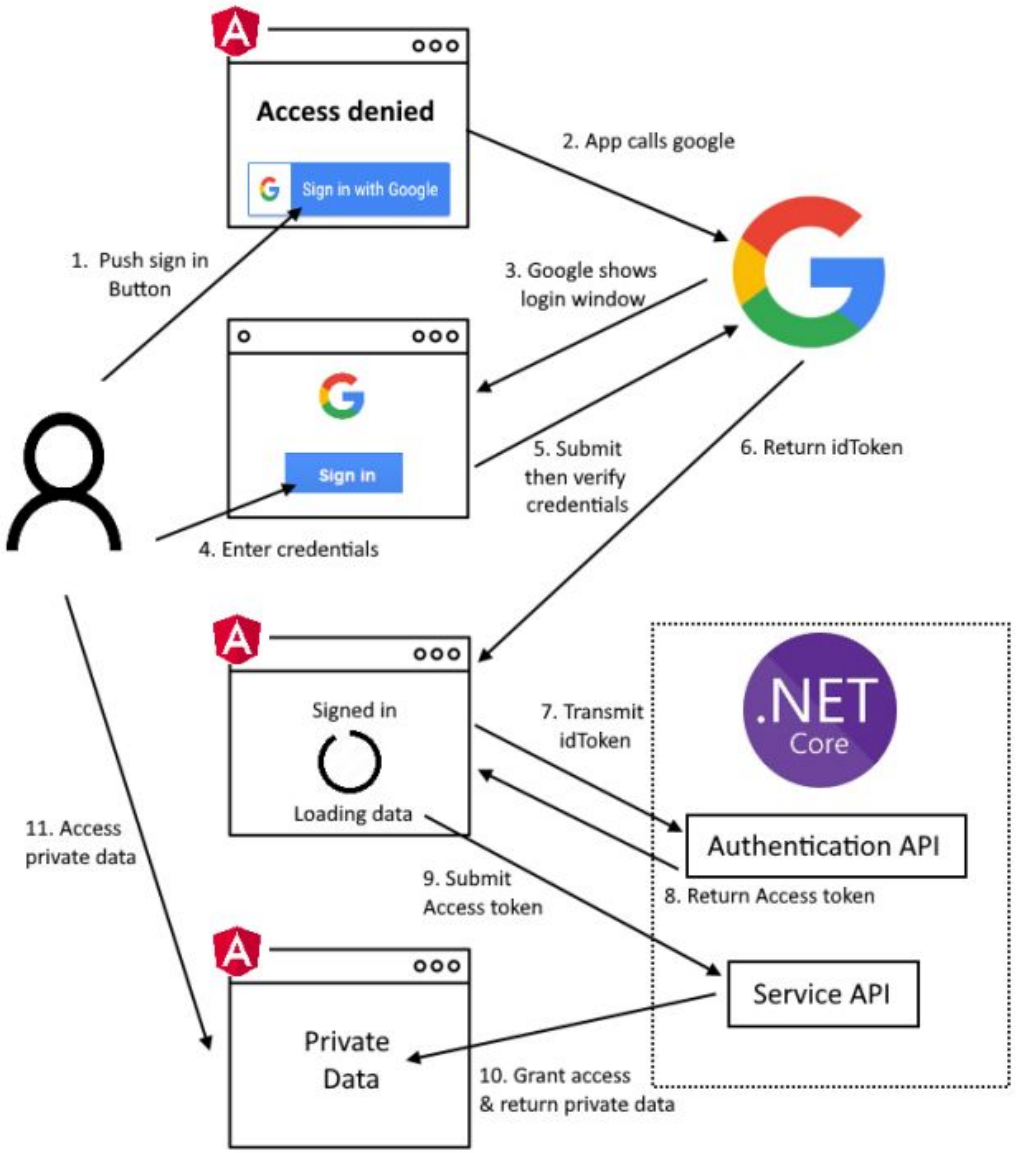
okta

Full Example



Rakamin

Full Example



Rakamin

TERIMA KASIH