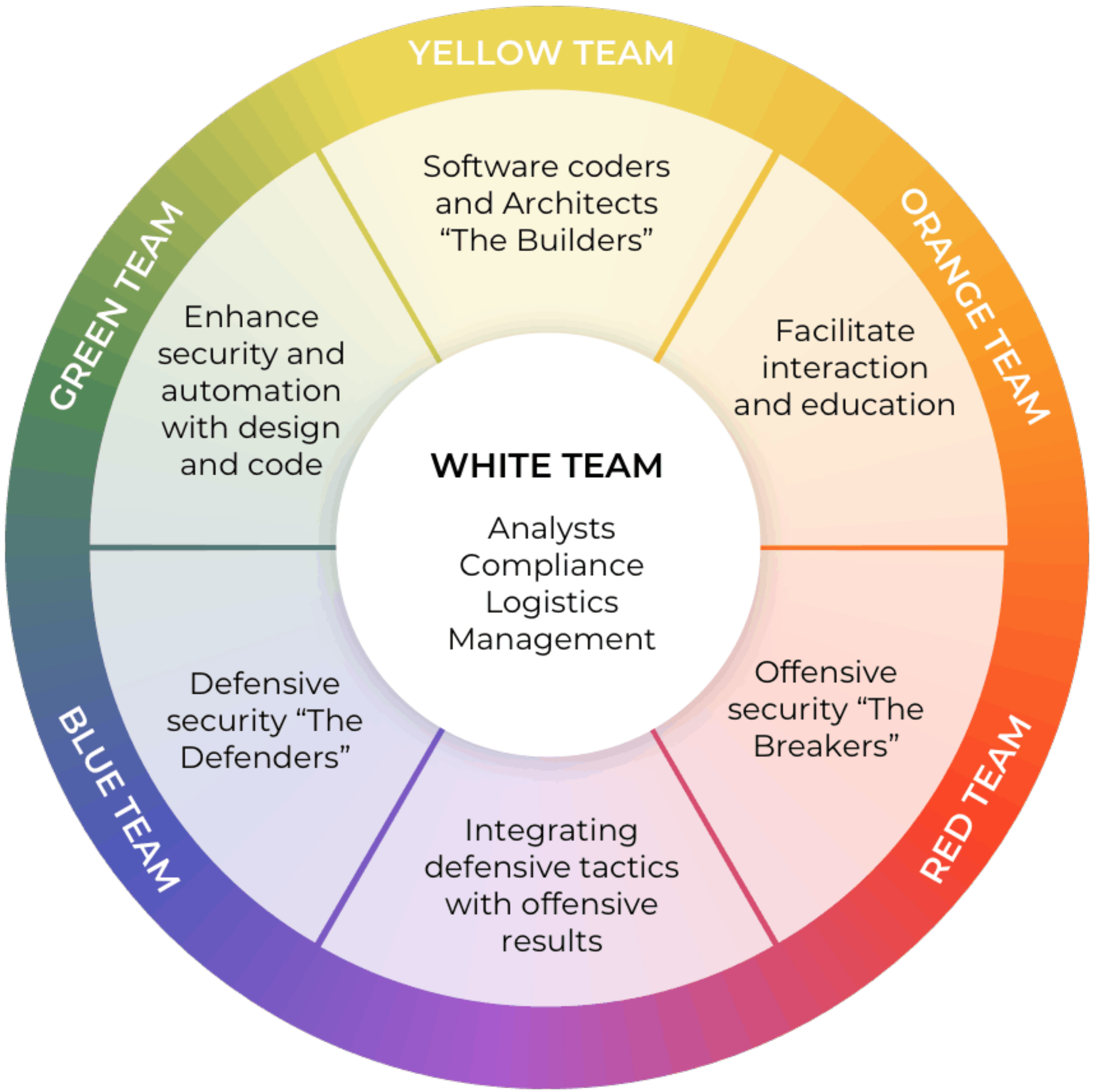
YELLOW TEAMING - II



YELLOW TEAM

Software coders and Architects “The Builders”

ORANGE TEAM

Facilitate interaction and education

RED TEAM

Offensive security “The Breakers”

Integrating defensive tactics with offensive results

BLUE TEAM

Defensive security “The Defenders”

GREEN TEAM

Enhance security and automation with design and code

WHITE TEAM

Analysts
Compliance
Logistics
Management

YELLOW TEAM

- Software Builders
- Application Developers
- Software Engineers
- System Architects

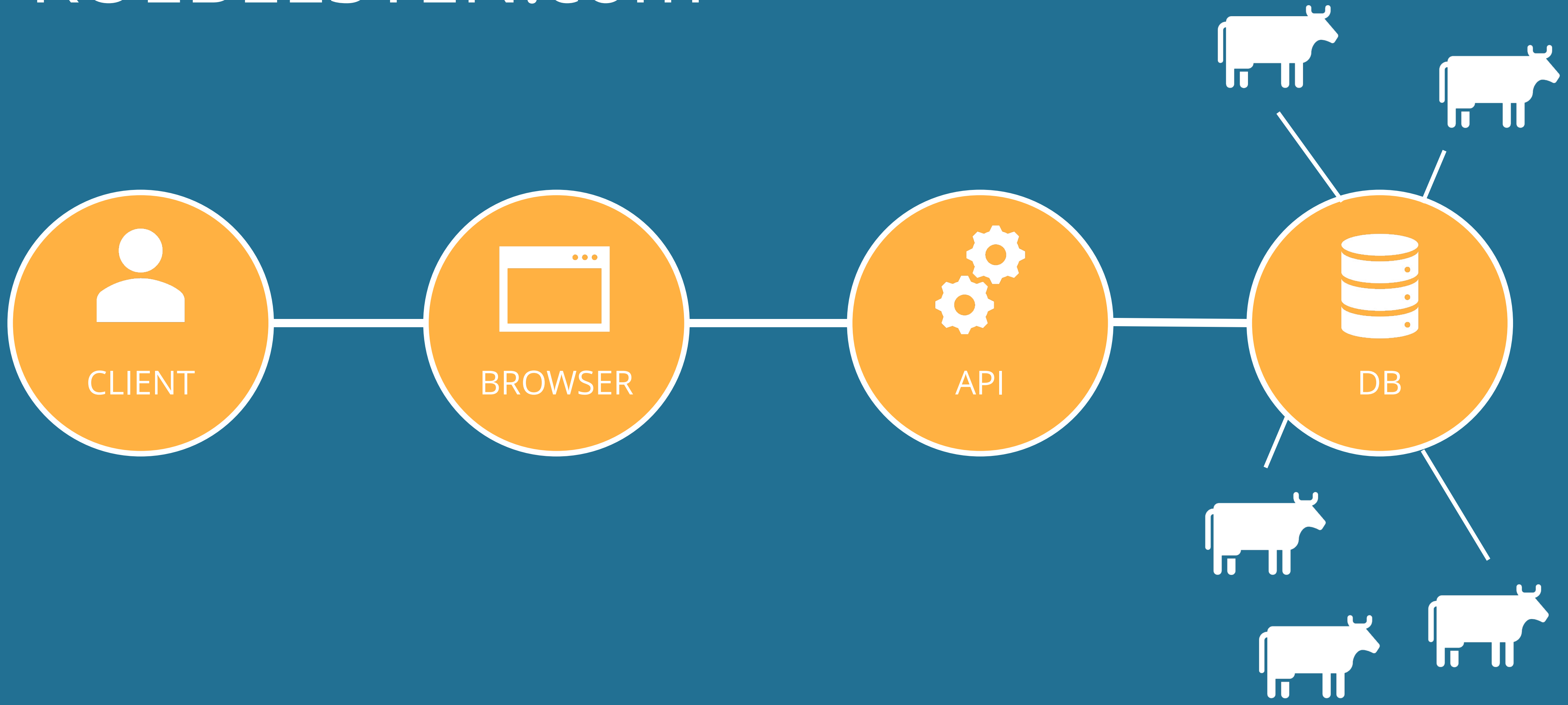
INPUT SANITIZATION

DON’T TRUST THE CLIENT

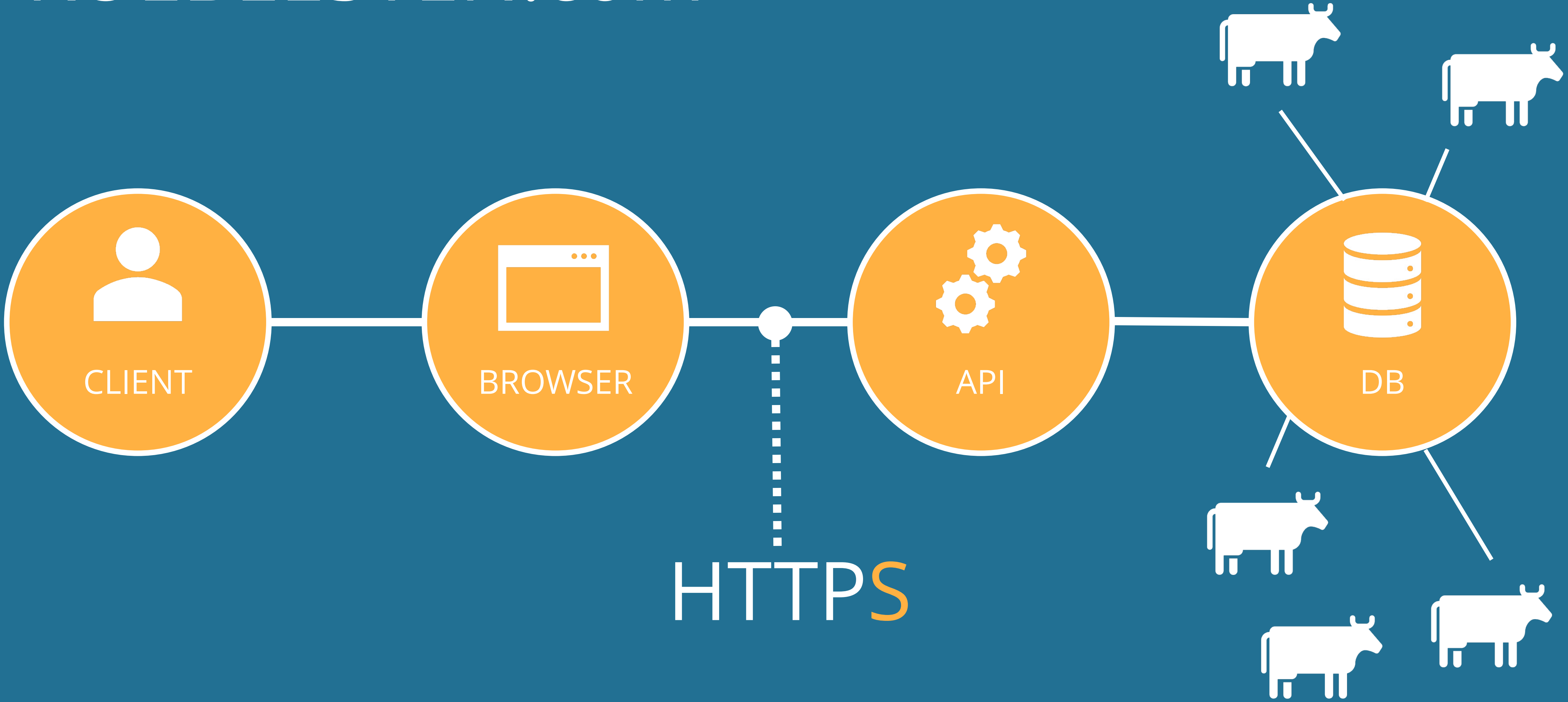
UPDATE YOUR SHIT

Wijsheid van Beckers™

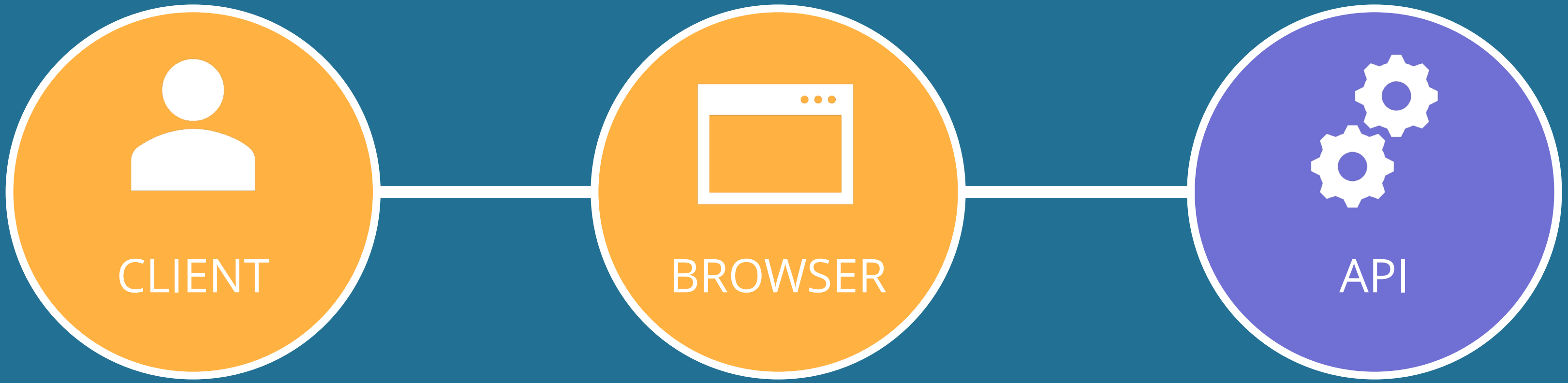
KOEBEESTEN.com



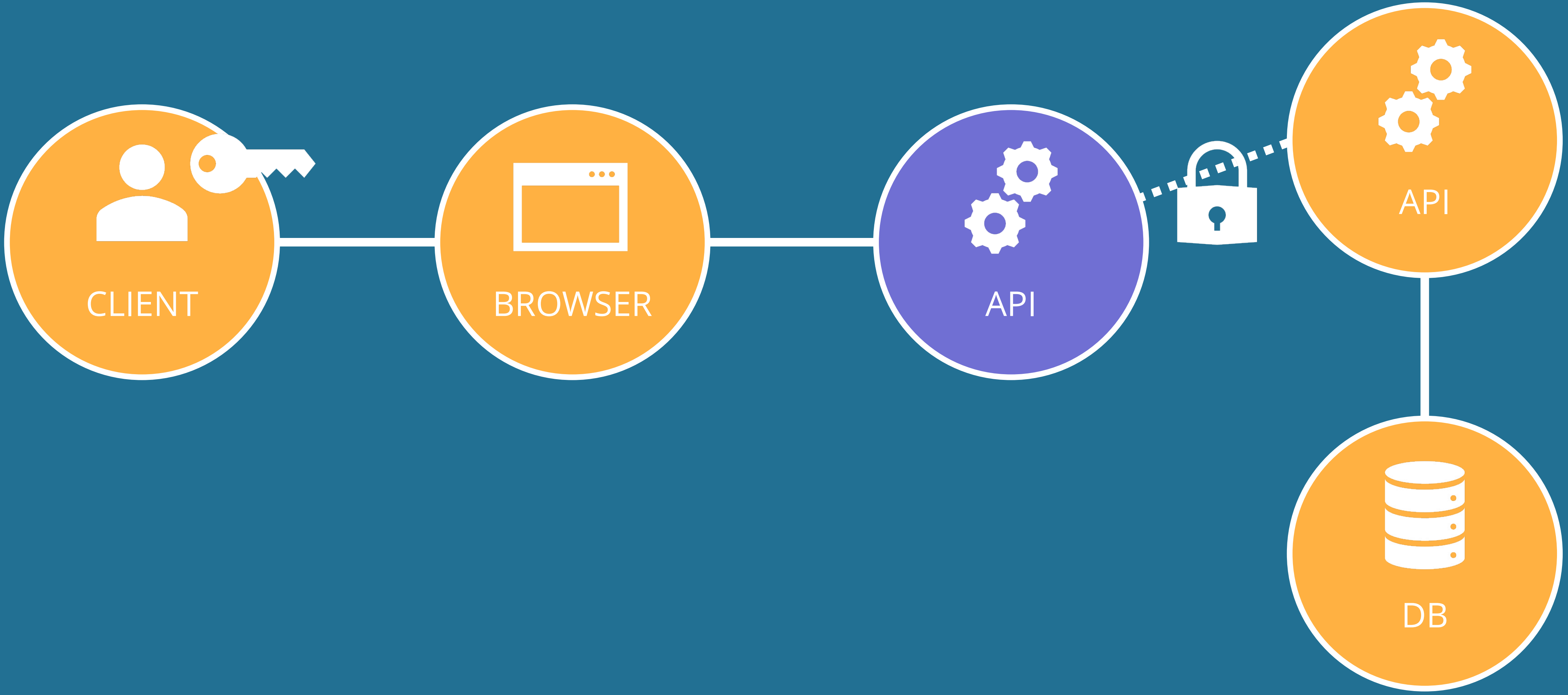
KOEBEESTEN.com



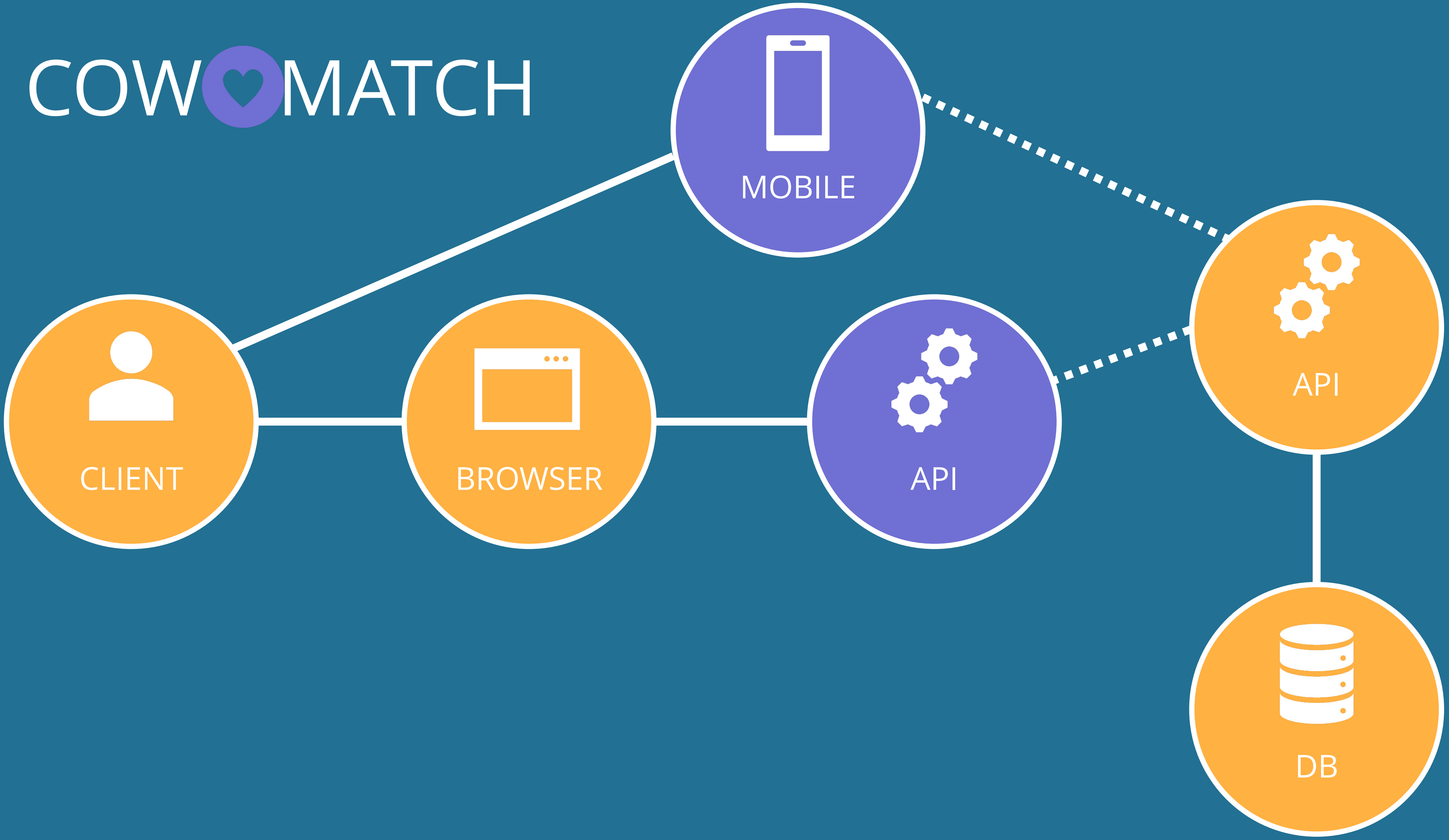
COW♥MATCH



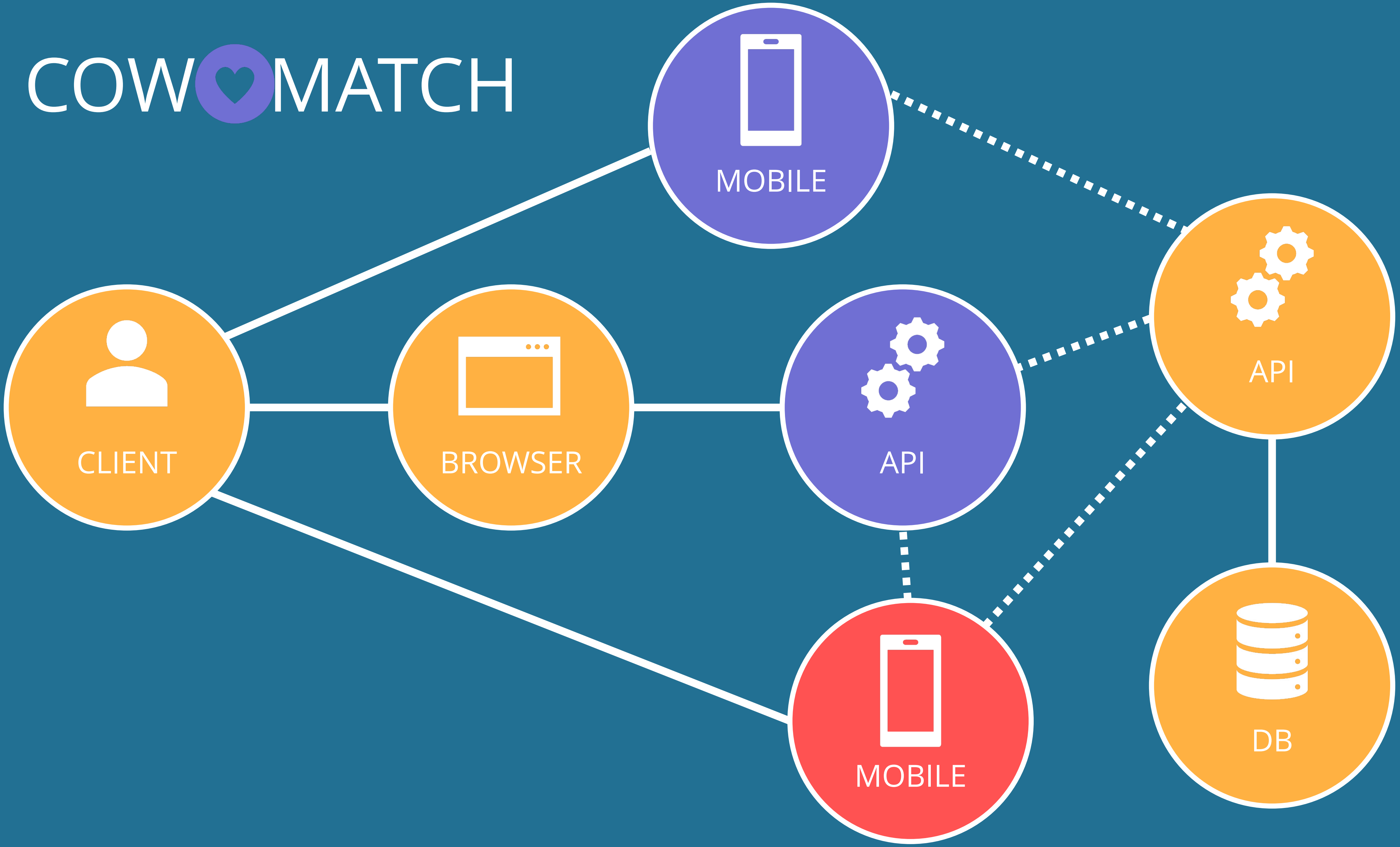
COW♥MATCH



COW♥MATCH



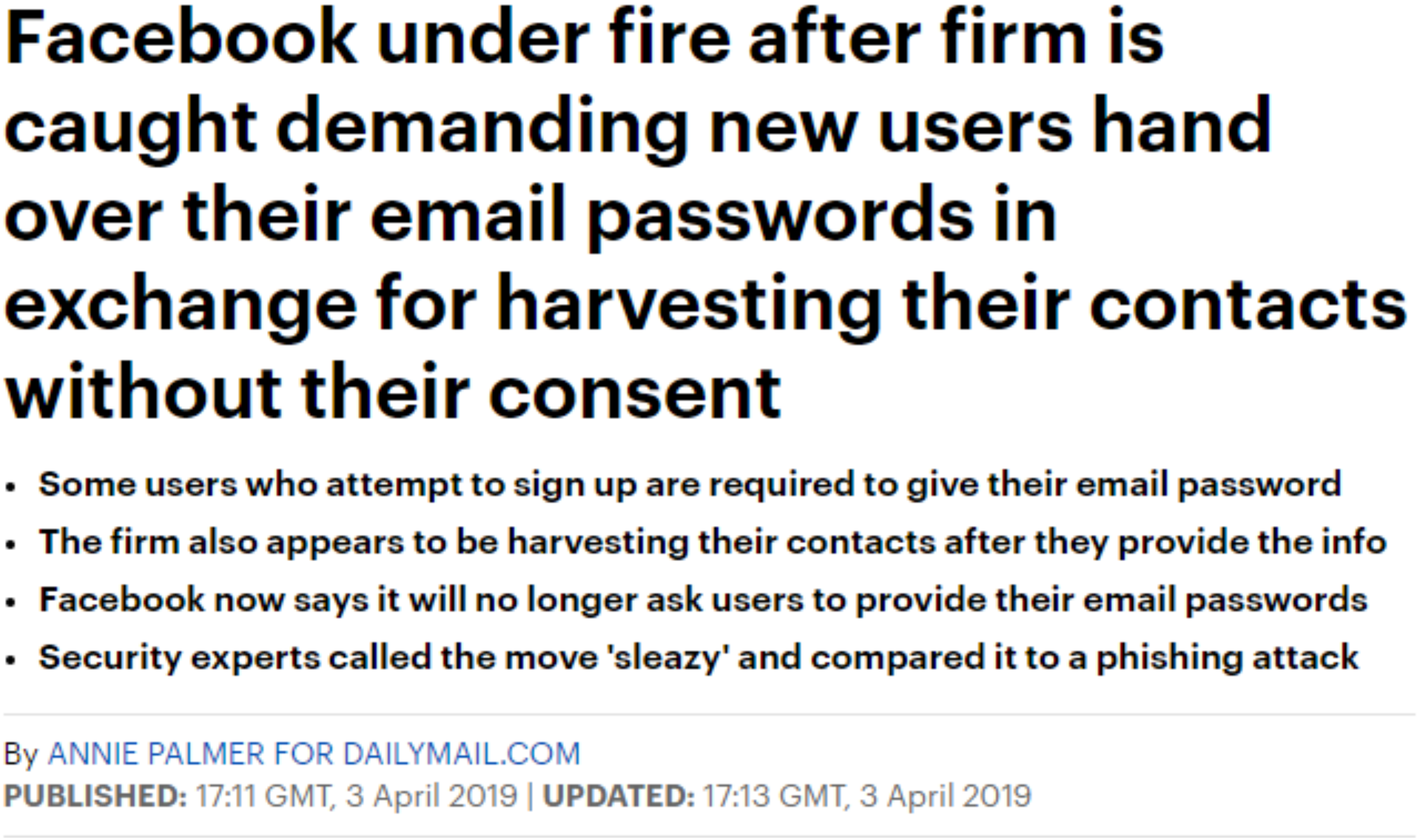
COW♥MATCH



THE PLAYERS

- Mobile / Native
- Single page applications
- Web API
- Fat Clients
- (Micro) services
- …

MACHINES COMMUNICATING ON BEHALF OF HUMANS



Facebook under fire after firm is caught demanding new users hand over their email passwords in exchange for harvesting their contacts without their consent

- Some users who attempt to sign up are required to give their email password
- The firm also appears to be harvesting their contacts after they provide the info
- Facebook now says it will no longer ask users to provide their email passwords
- Security experts called the move 'sleazy' and compared it to a phishing attack

By ANNIE PALMER FOR DAILYMAIL.COM
PUBLISHED: 17:11 GMT, 3 April 2019 | **UPDATED:** 17:13 GMT, 3 April 2019

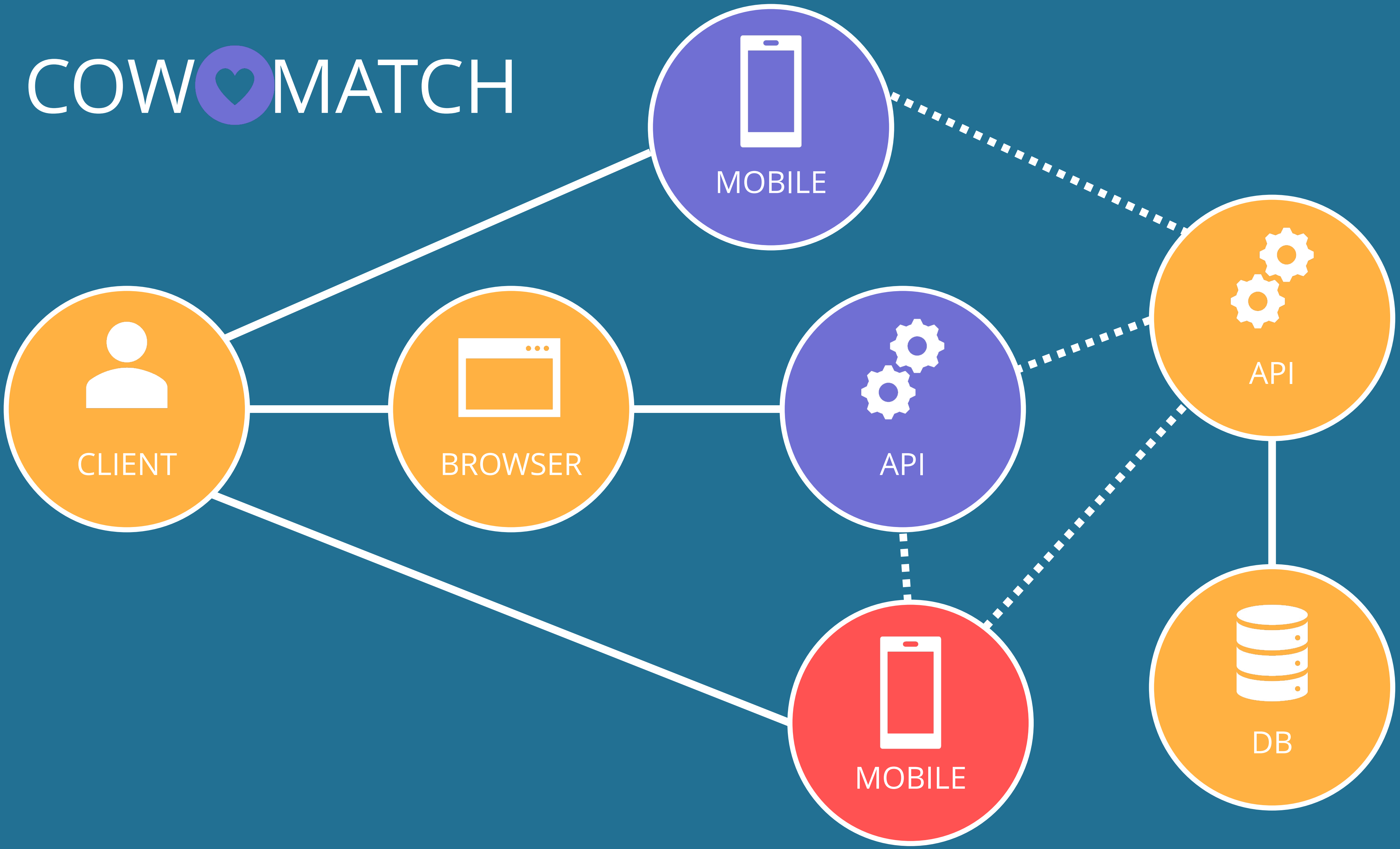
COOKIES?

API KEY!

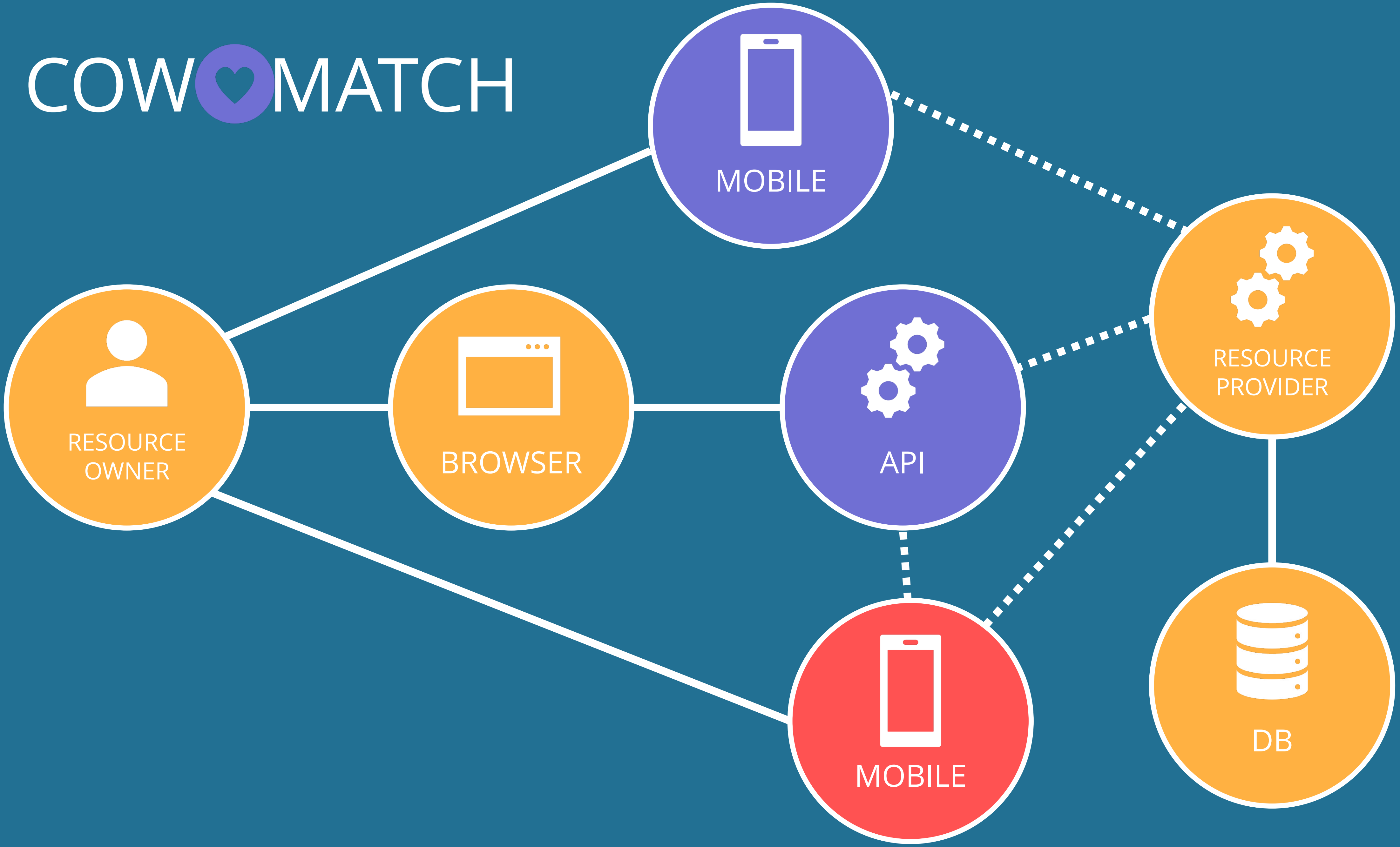
API KEY?

SSO!

COW♥MATCH



COW♥MATCH

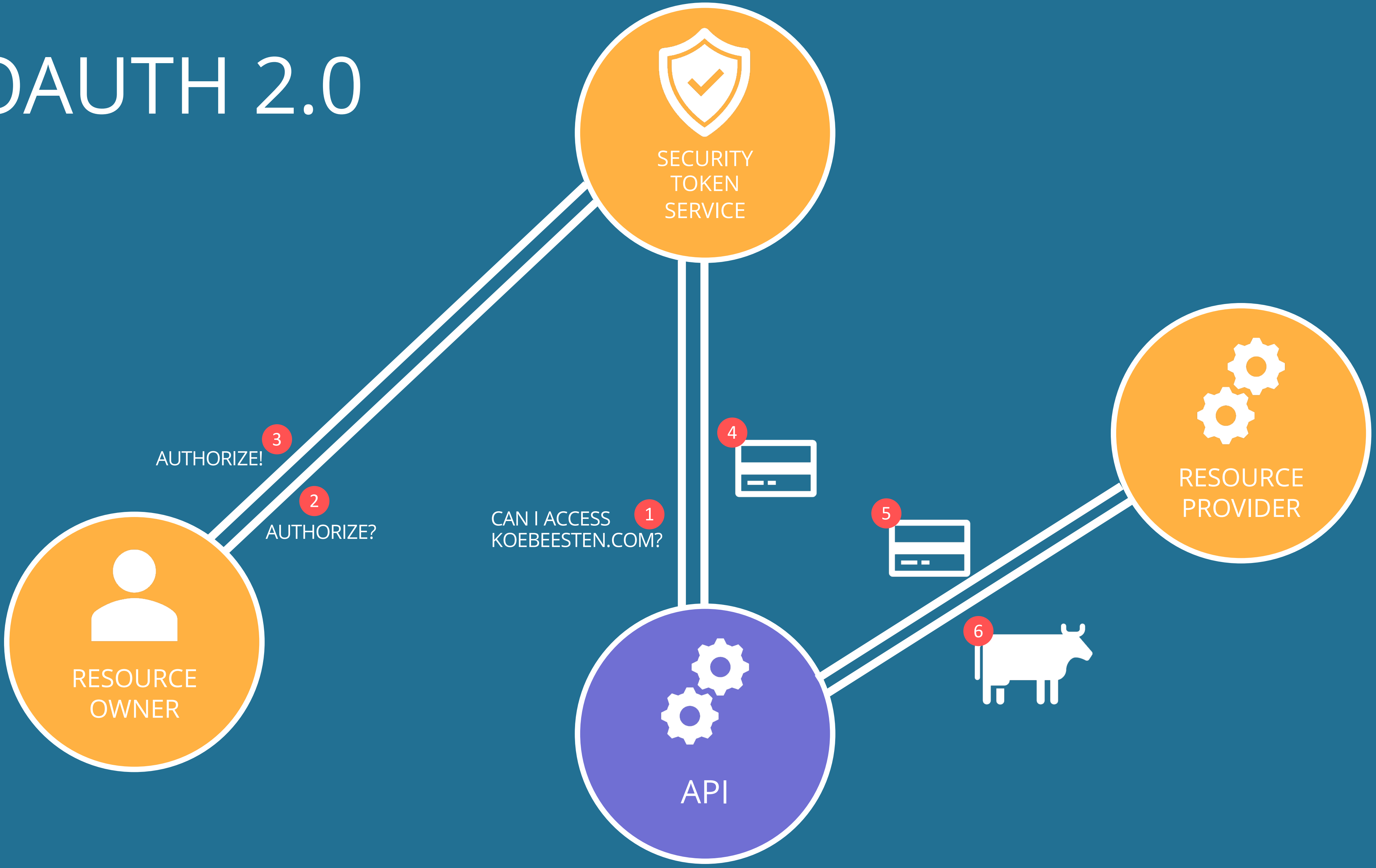

MOBILE
RESOURCE OWNER
BROWSER
API
RESOURCE PROVIDER
MOBILE
DB

OAUTH 2.0

SECURITY
TOKEN
SERVICE

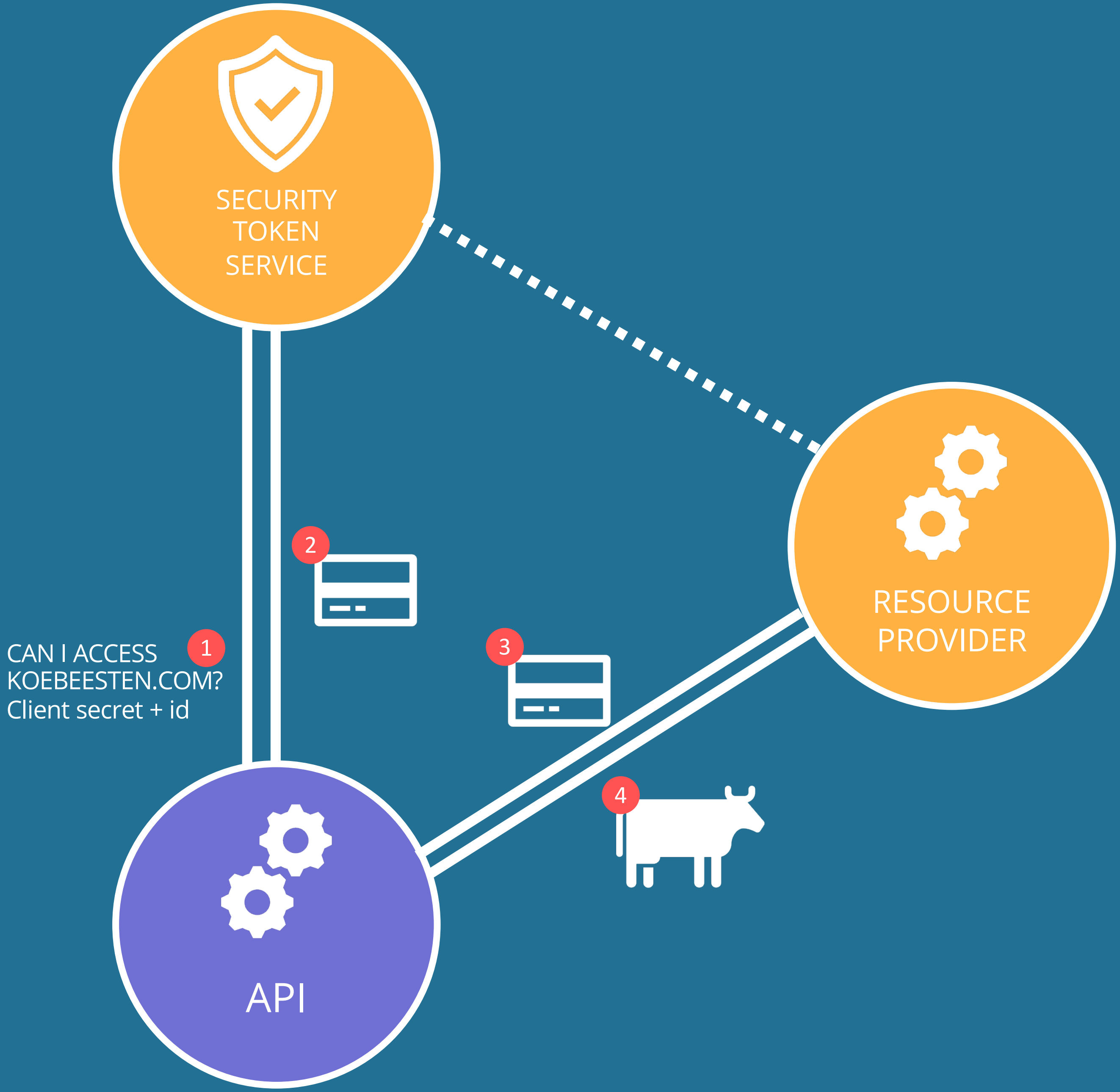
- Centralized Authorization Management
- Updates (Policies)
- Single point of failure?

OAUTH 2.0

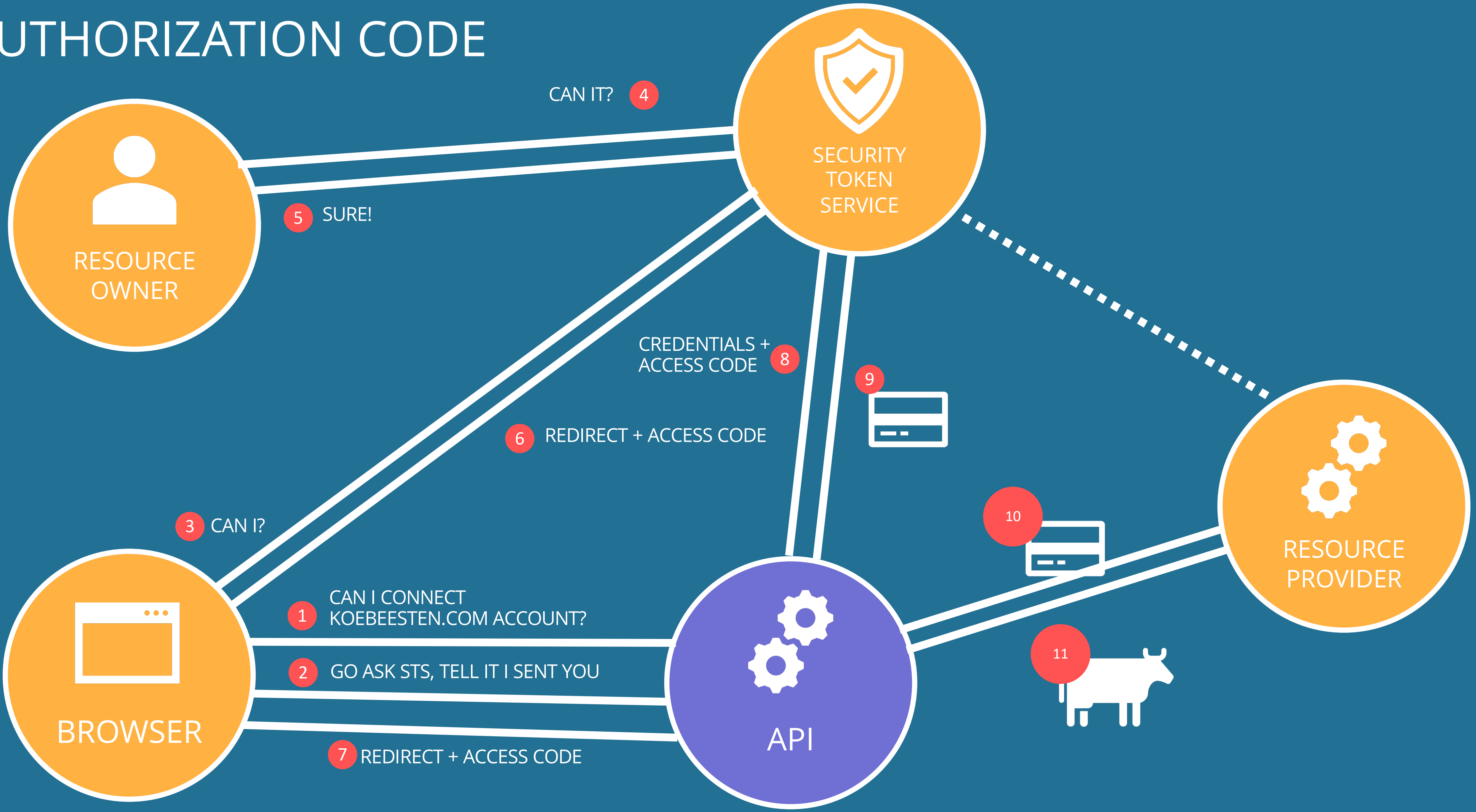

SECURITY
TOKEN
SERVICE
3
AUTHORIZE!
2
AUTHORIZE?
CAN I ACCESS
KOEBEESTEN.COM?
1
4
5
RESOURCE
PROVIDER
6
RESOURCE
OWNER
API

CLIENT CREDENTIALS

Machine-to-machine



AUTHORIZATION CODE

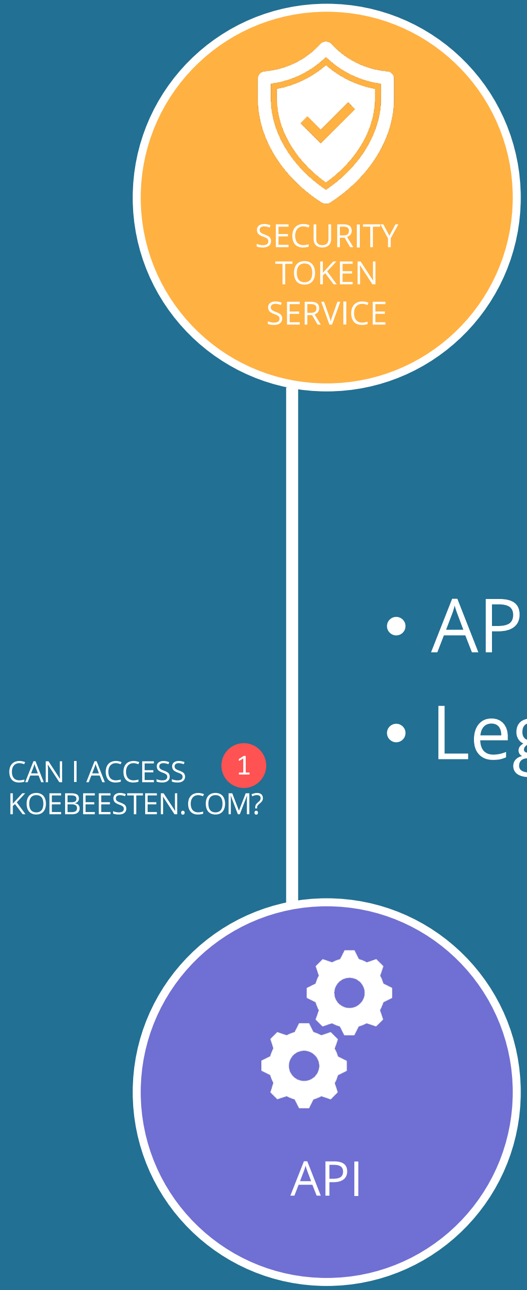


- JWT Token (jwt.io)
- Bearer Token! HTTPS is crucial!
- What about Mobile?
- What about SPAs?
- What about Authentication?
- Expiration
- Signature
- Scope

SECURITY
TOKEN
SERVICE

- Roll your own (please don’t)
- Use existing services (Auth0)
- Use middleware
- Use a public STS

OAUTH 2.0



- API needs to be registered
- Legitimate redirect URI

INPUT SANITIZATION

DON’T TRUST THE CLIENT

UPDATE YOUR SHIT

Wijsheid van Beckers™

- https://pragmaticwebsecurity.com/courses/introduction-oauth-oidc.html

- Getting Started with ASP.NET Core and Oauth
  https://app.pluralsight.com/library/courses/asp-dot-net-core-oauth

- Securing ASP.NET Core 3 With OAuth2 and OpenID Connect
  https://app.pluralsight.com/library/courses/securing-aspnet-core-3-oauth2-openid-connect