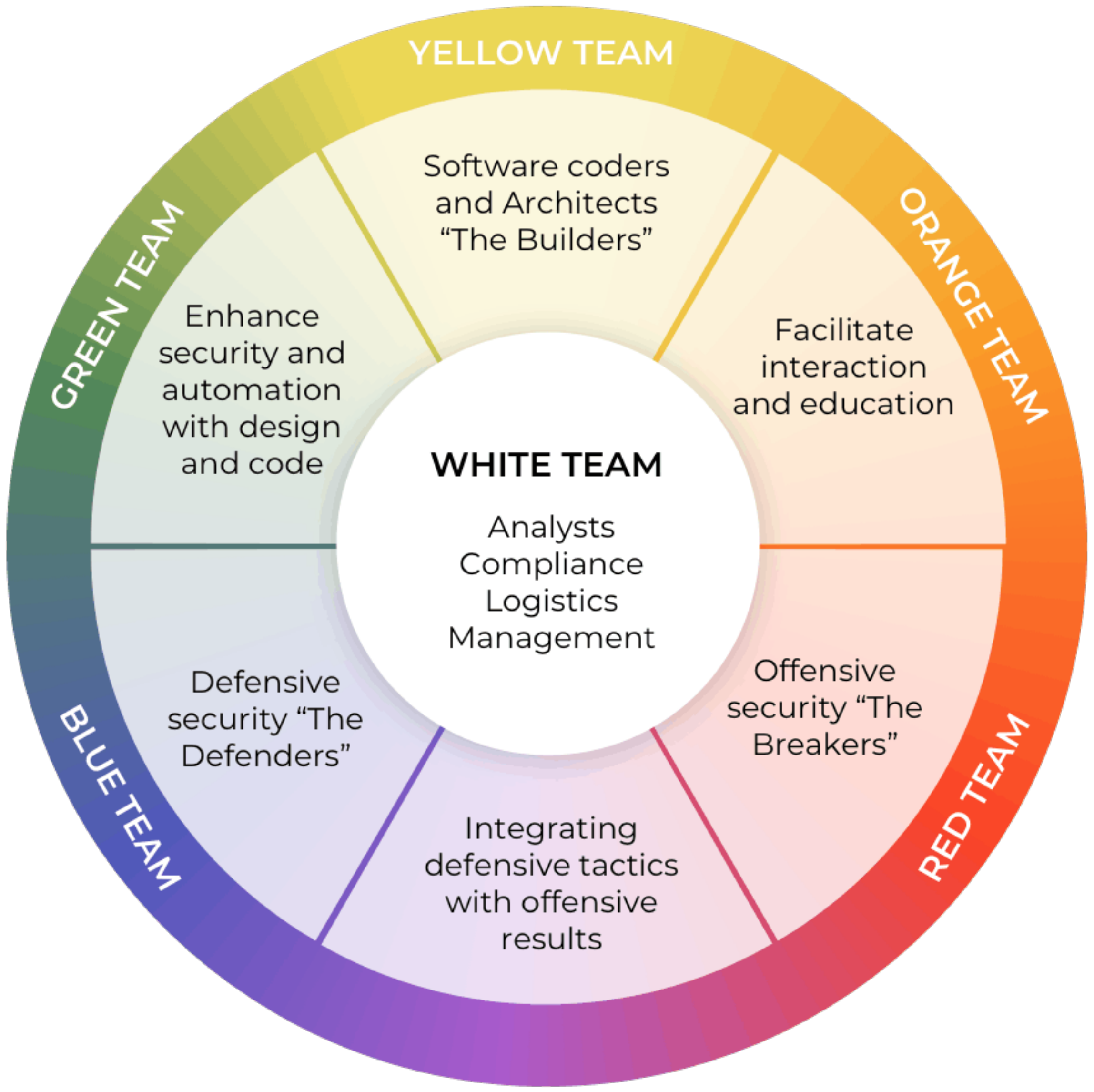
YELLOW TEAMING - III


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

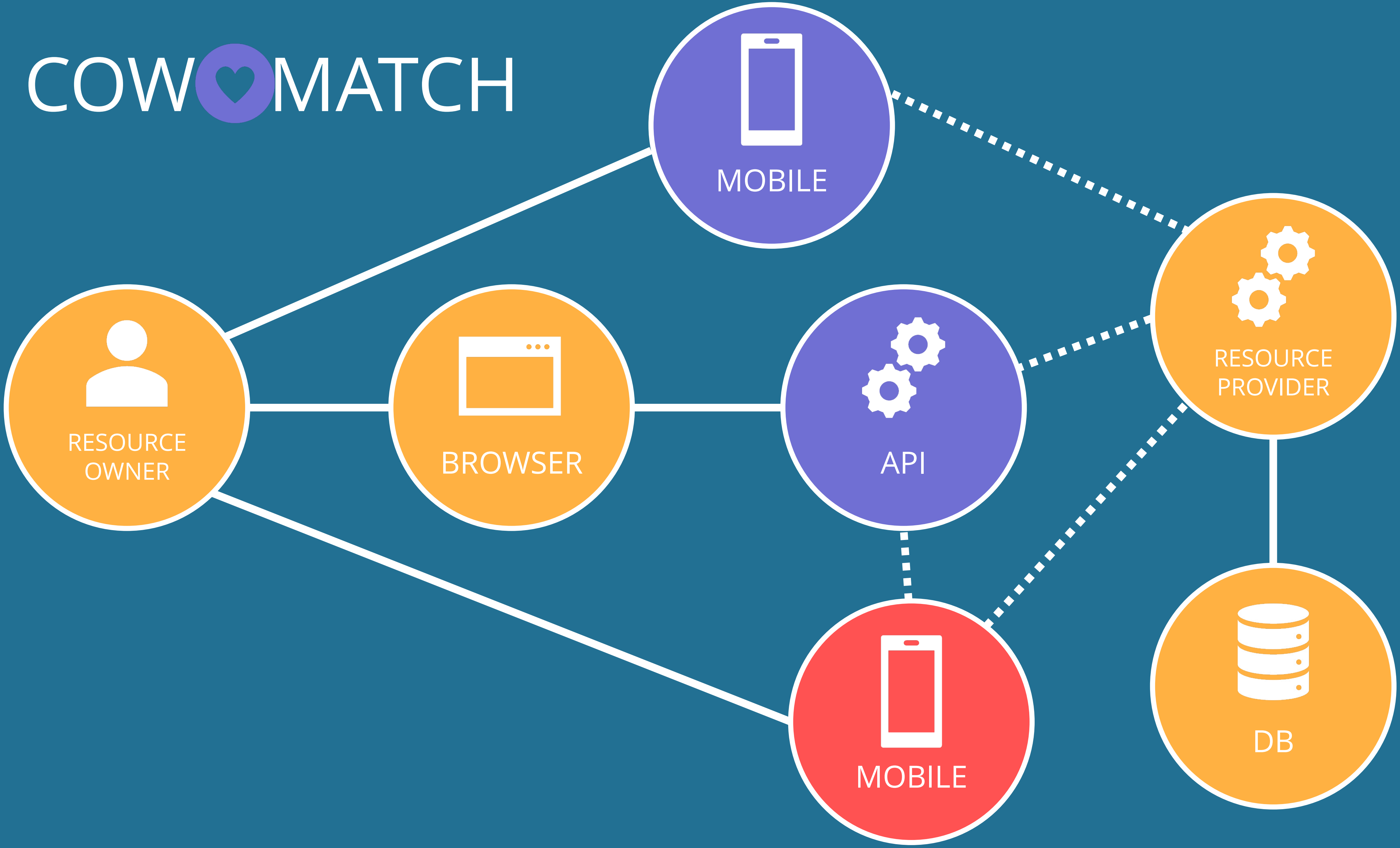
INPUT SANITIZATION

DON’T TRUST THE CLIENT

UPDATE YOUR SHIT

Wijsheid van Beckers™

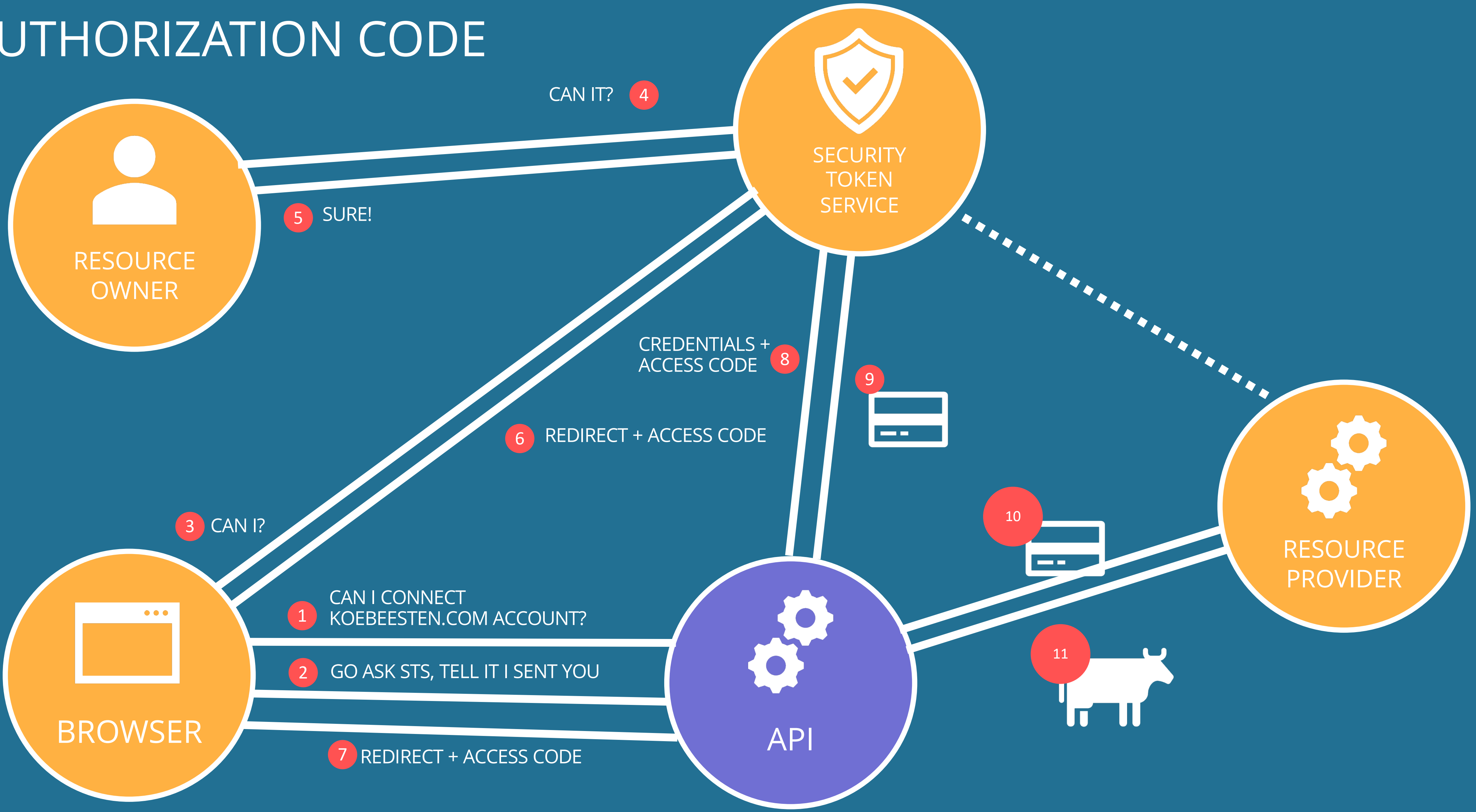
COWMATCH


MOBILE
RESOURCE OWNER
BROWSER
API
RESOURCE PROVIDER
MOBILE
DB

MACHINES COMMUNICATING ON BEHALF OF HUMANS

SSO!

AUTHORIZATION CODE

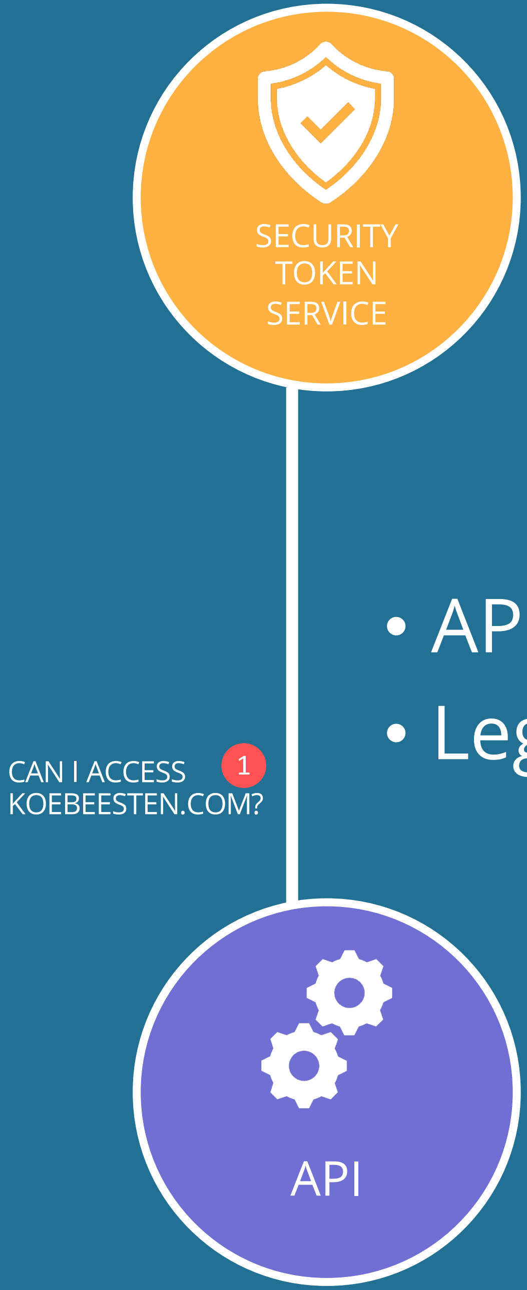


SECURITY
TOKEN
SERVICE

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

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

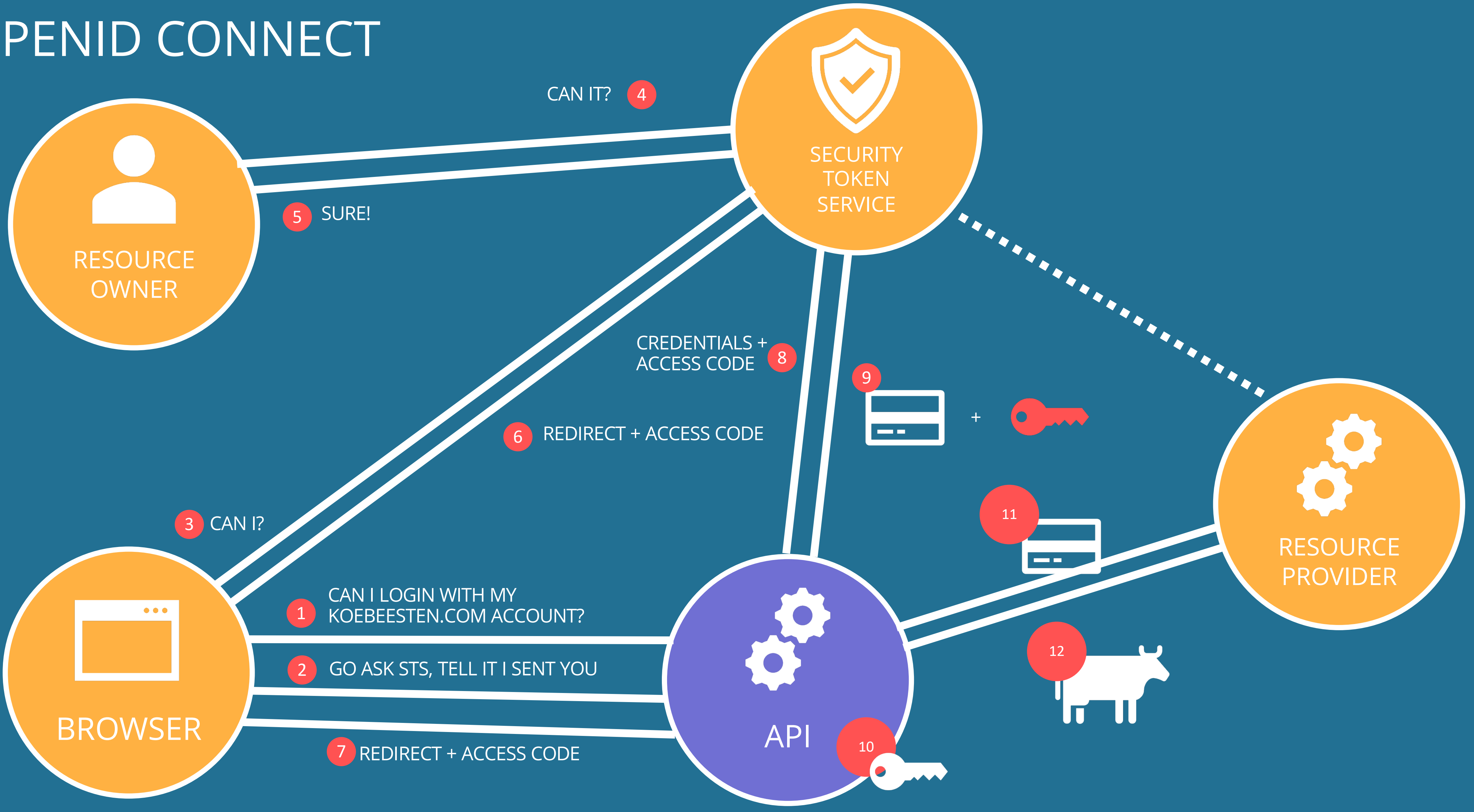
OAUTH 2.0



- API needs to be registered
- Legitimate redirect URI

OAUTH 2.0 FOR AUTHENTICATION

OPENID CONNECT



MOBILE

- Cannot be trusted
- Client secret
- Redirect URI

MOBILE

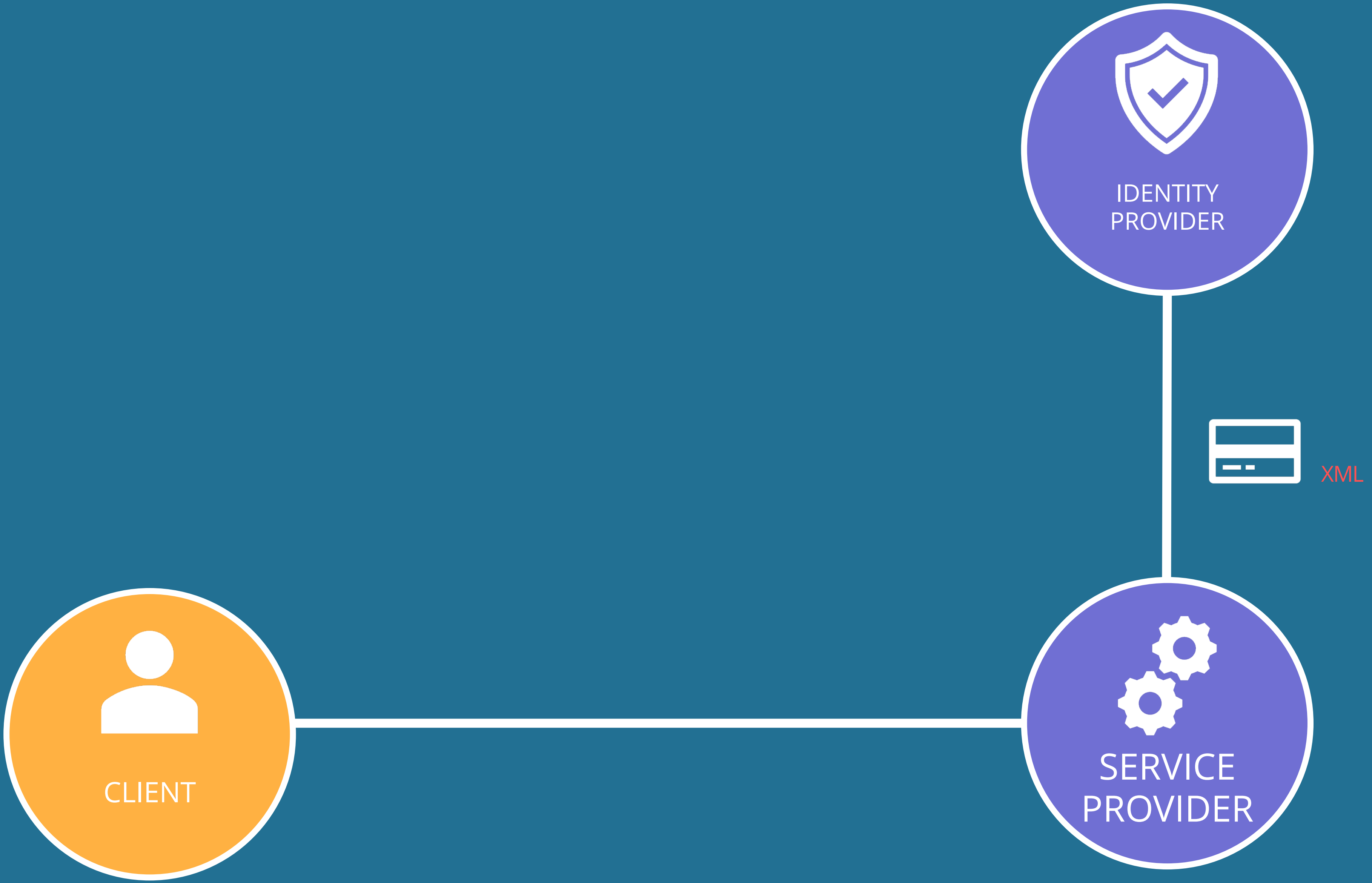
Proof Key for Code Exchange

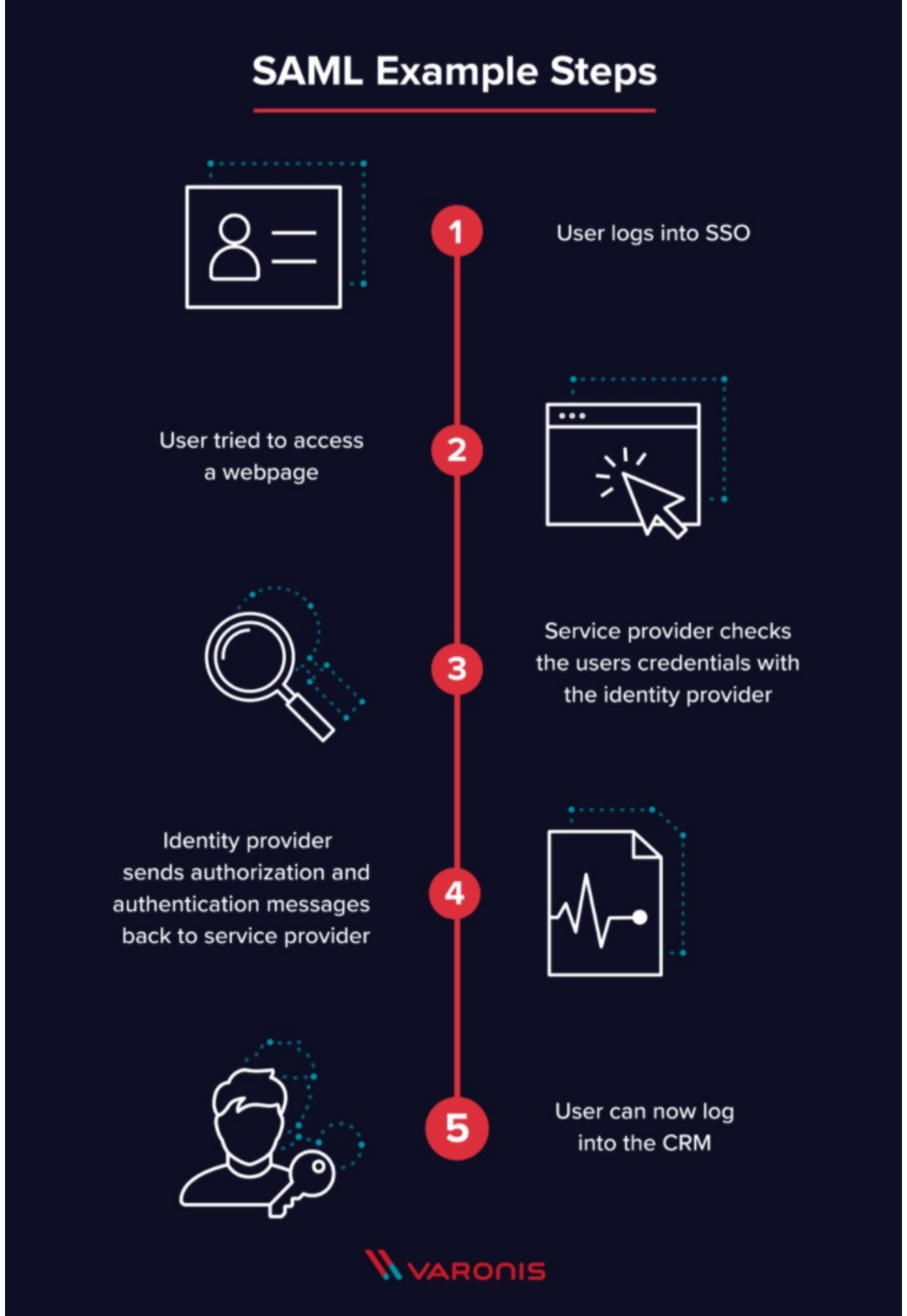
Code Challenge = SHA256(Code verifier)

- Generate code verifier and code challenge
- Code challenge used in front channel
- Code verifier used instead of client credentials
- STS gets code challenge from client, code verifier from api
- Maybe we should do this all the time?

SPA

SAML!


IDENTITY PROVIDER
XML
CLIENT
SERVICE PROVIDER



SAML Example Steps

1. User logs into SSO
2. User tried to access a webpage
3. Service provider checks the users credentials with the identity provider
4. Identity provider sends authorization and authentication messages back to service provider
5. User can now log into the CRM

VARONIS

SAML!

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