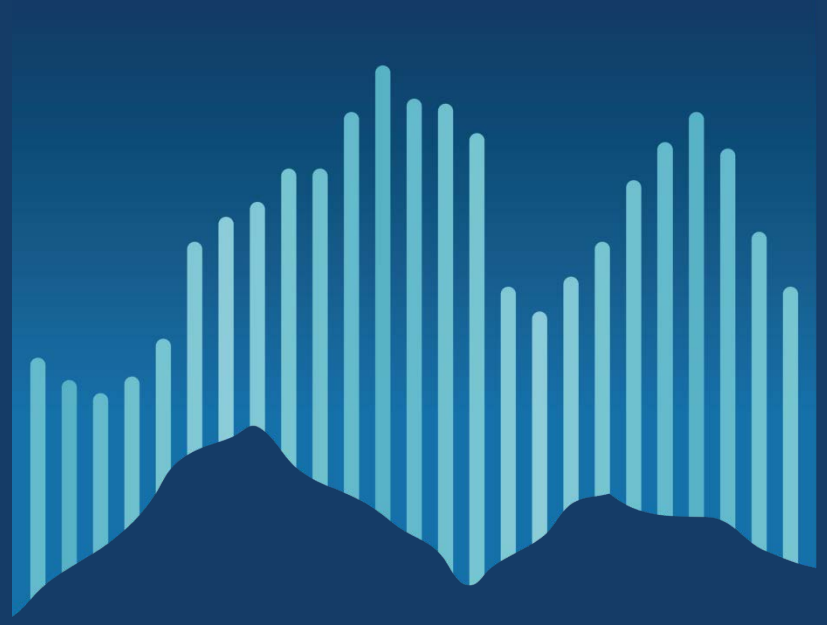
CURITY

Secure your APIs & Microservices with OAuth & OpenID Connect

By Travis Spencer, CEO
@travisspencer, @curityio

Copyright © 2018 Curity AB



NORDIC **APIS**

Organizers and founders

- ✓ All API Conferences
- ✓ API Community
- ✓ Active blogosphere

Austin API Summit
June 11 – 13 | Austin, Texas

2018 Platform Summit
October 22 - 24 | Stockholm, Sweden

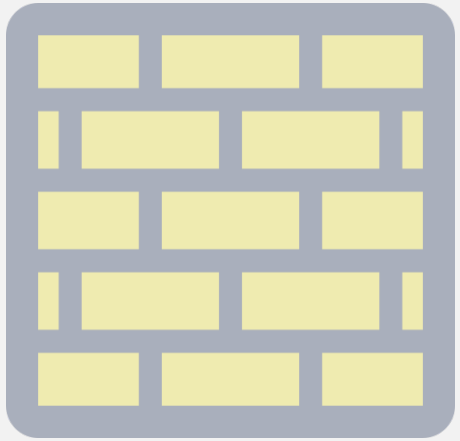
API Security == API Keys

- Problem Solved!

Copyright © 2018 Curity AB

API Security != API Keys

- Revocable, non-expiring, bearer access tokens
- Symmetric keys
- Passwords!



Copyright © 2018 Curity AB

API Security == OAuth

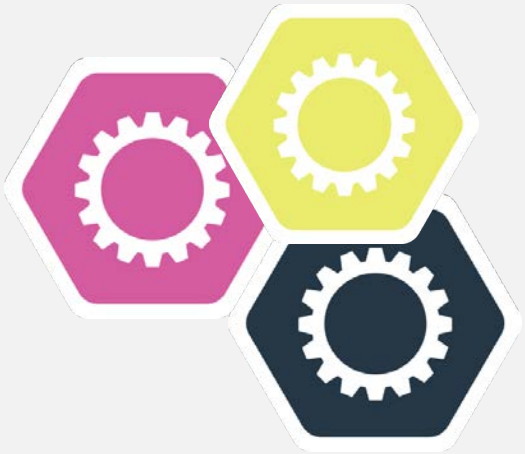
- Problem solved for real this time?

Not that easy! Sorry ☹

Copyright © 2018 Curity AB

Crucial Security Concerns

Enterprise Security

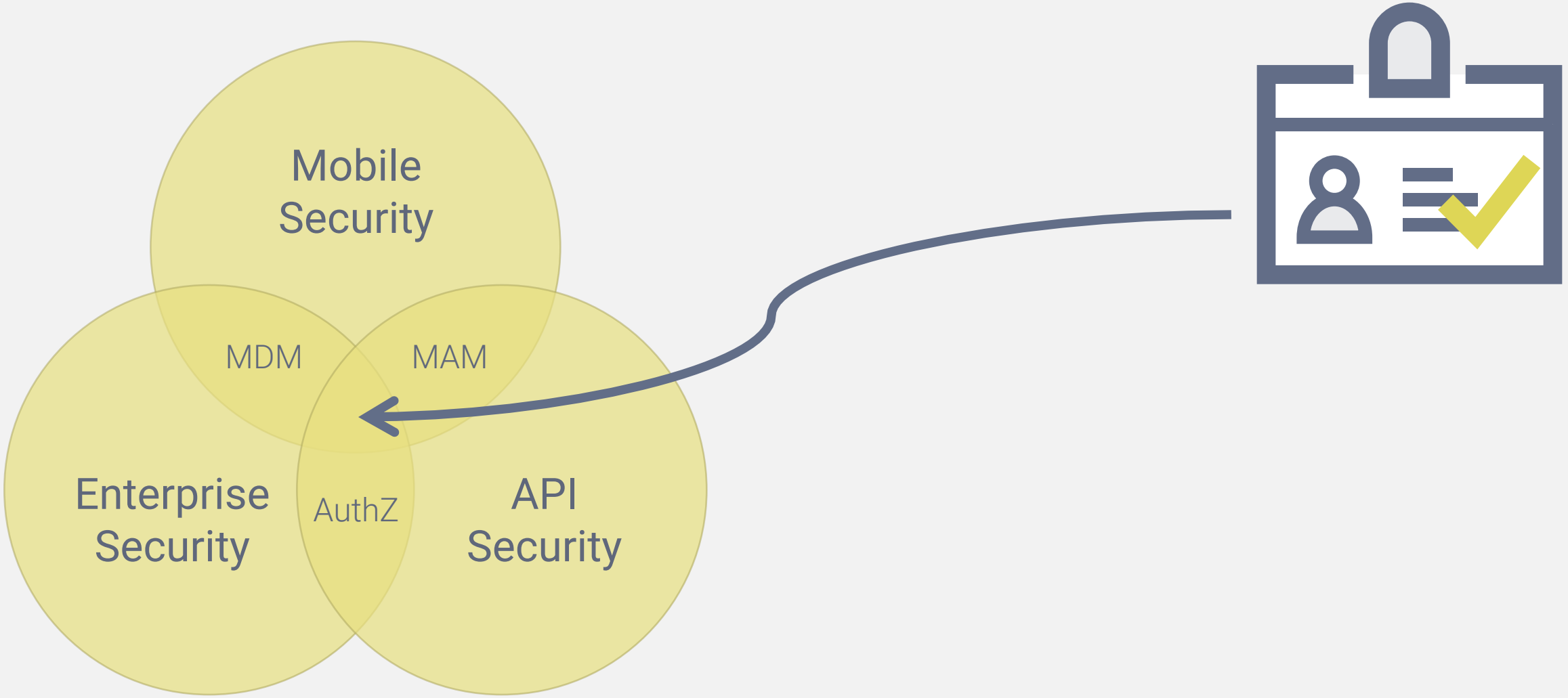


API Security

Mobile Security

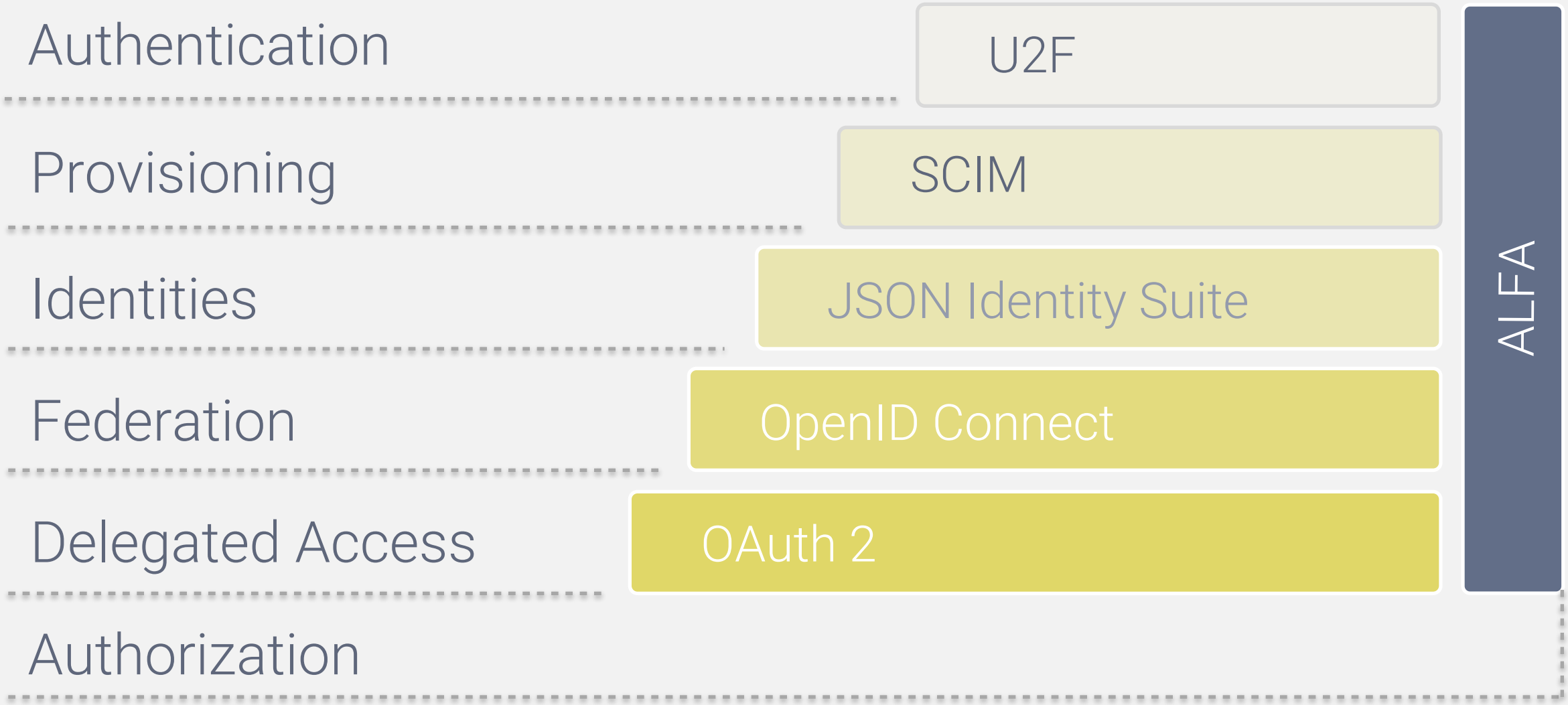
Copyright © 2018 Curity AB

Identity is Central



Copyright © 2018 Curity AB

The Neo-security Stack



Copyright © 2018 Curity AB

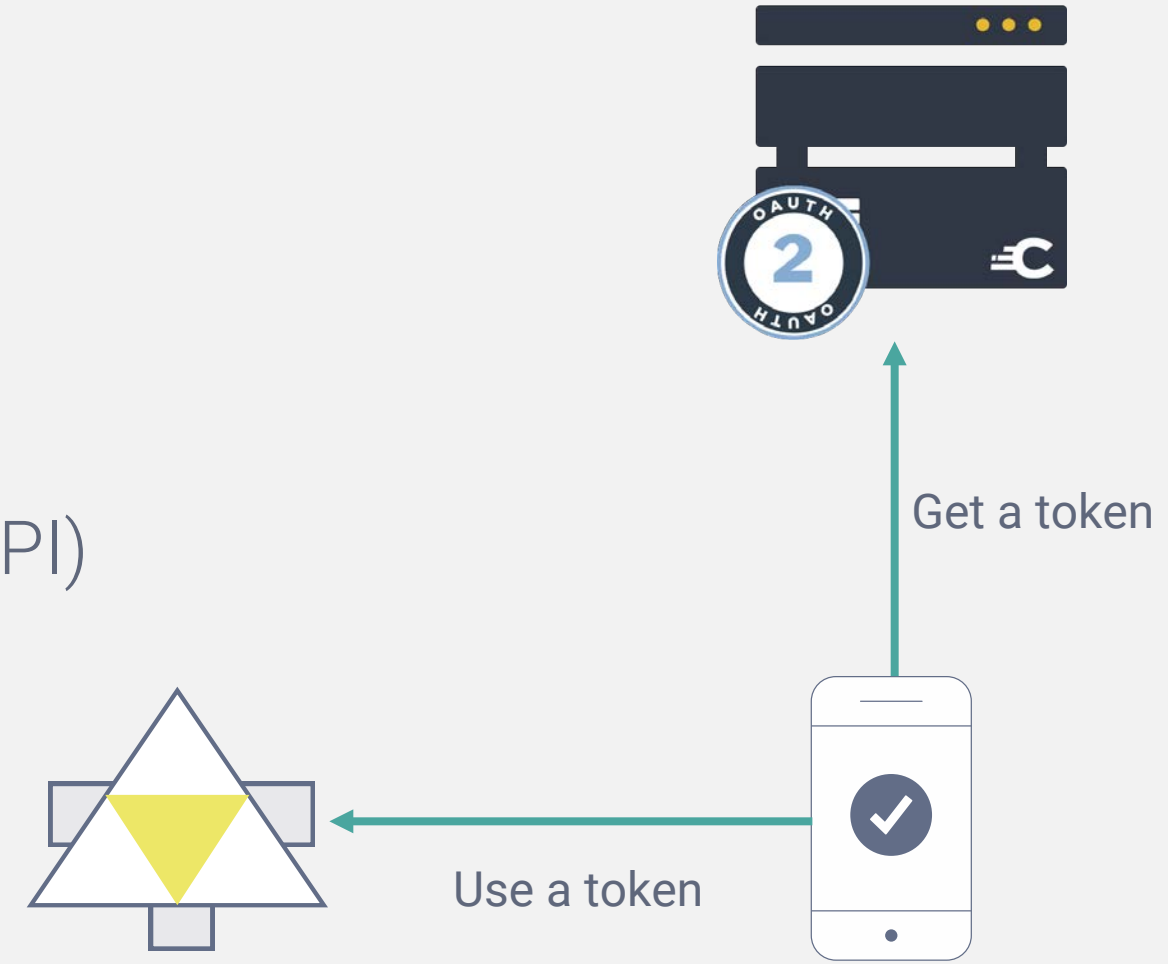
OAuth

- OAuth 2 is the new protocol of protocols
  - Used as the base of other specifications
  - OpenID Connect, UMA, HEART, etc.
- Addresses some important requirements
  - Delegated access
  - No password sharing
  - Revocation of access

Copyright © 2018 Curity AB

OAuth Actors

1. Resource Owner (RO)
2. Client
3. Authorization Server (AS)
4. Resource Server (RS) (i.e., API)



Copyright © 2018 Curity AB

Request, Authenticate & Consent

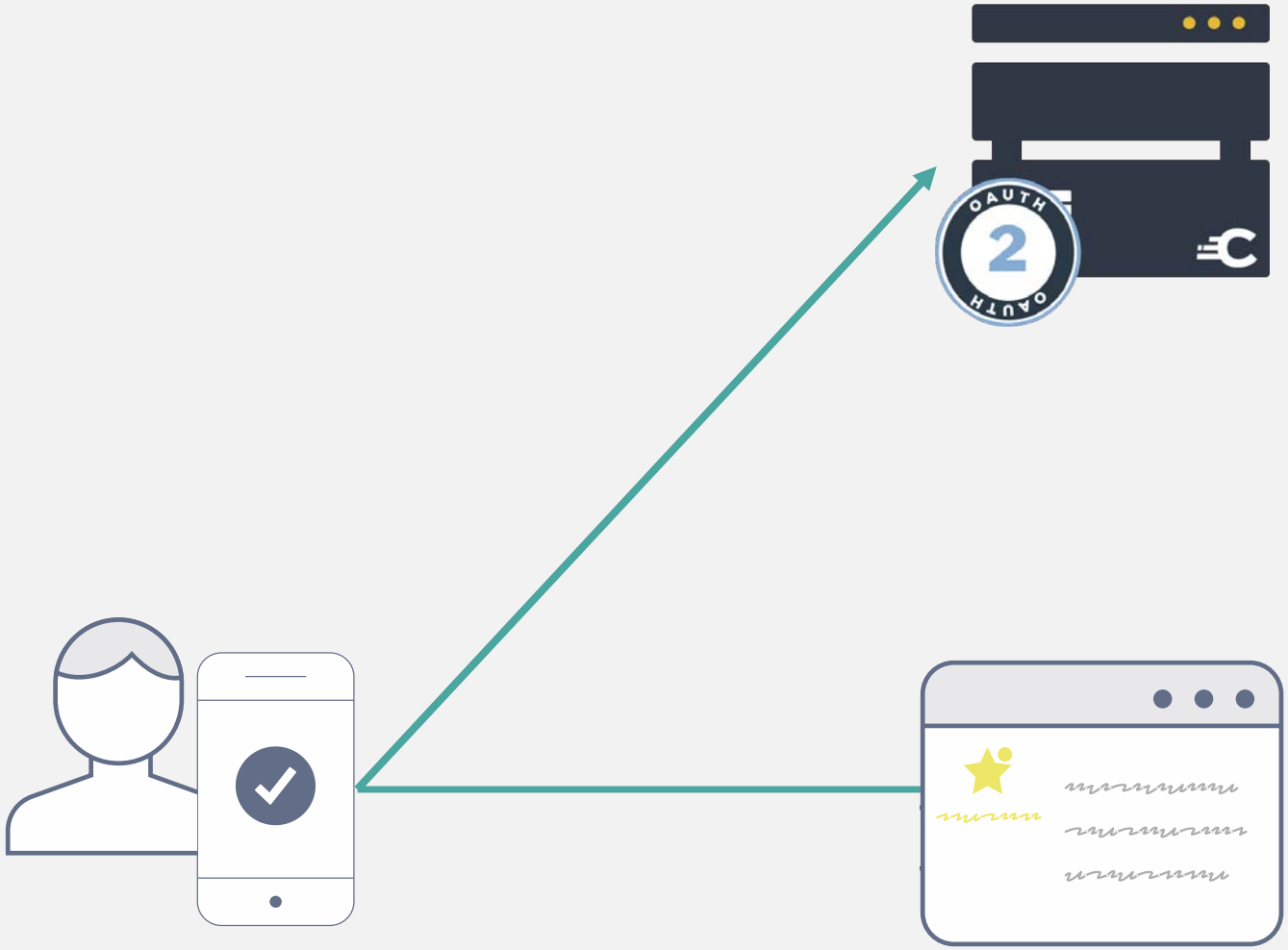
Request Access

Login

Consent

Copyright © 2018 Curity AB

Code Flow

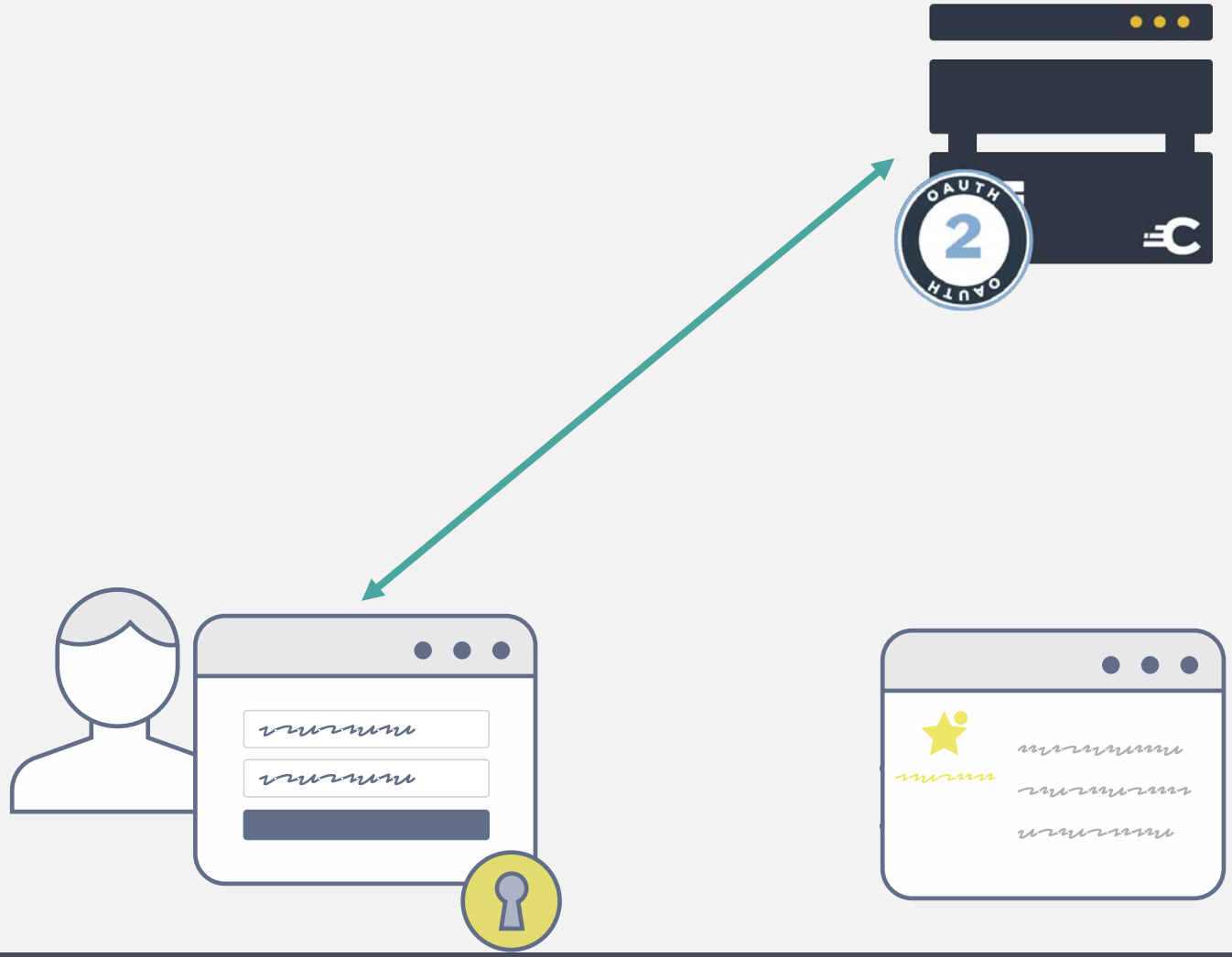


User is redirected to OAuth server

APIs & microservices

Copyright © 2018 Curity AB

Code Flow

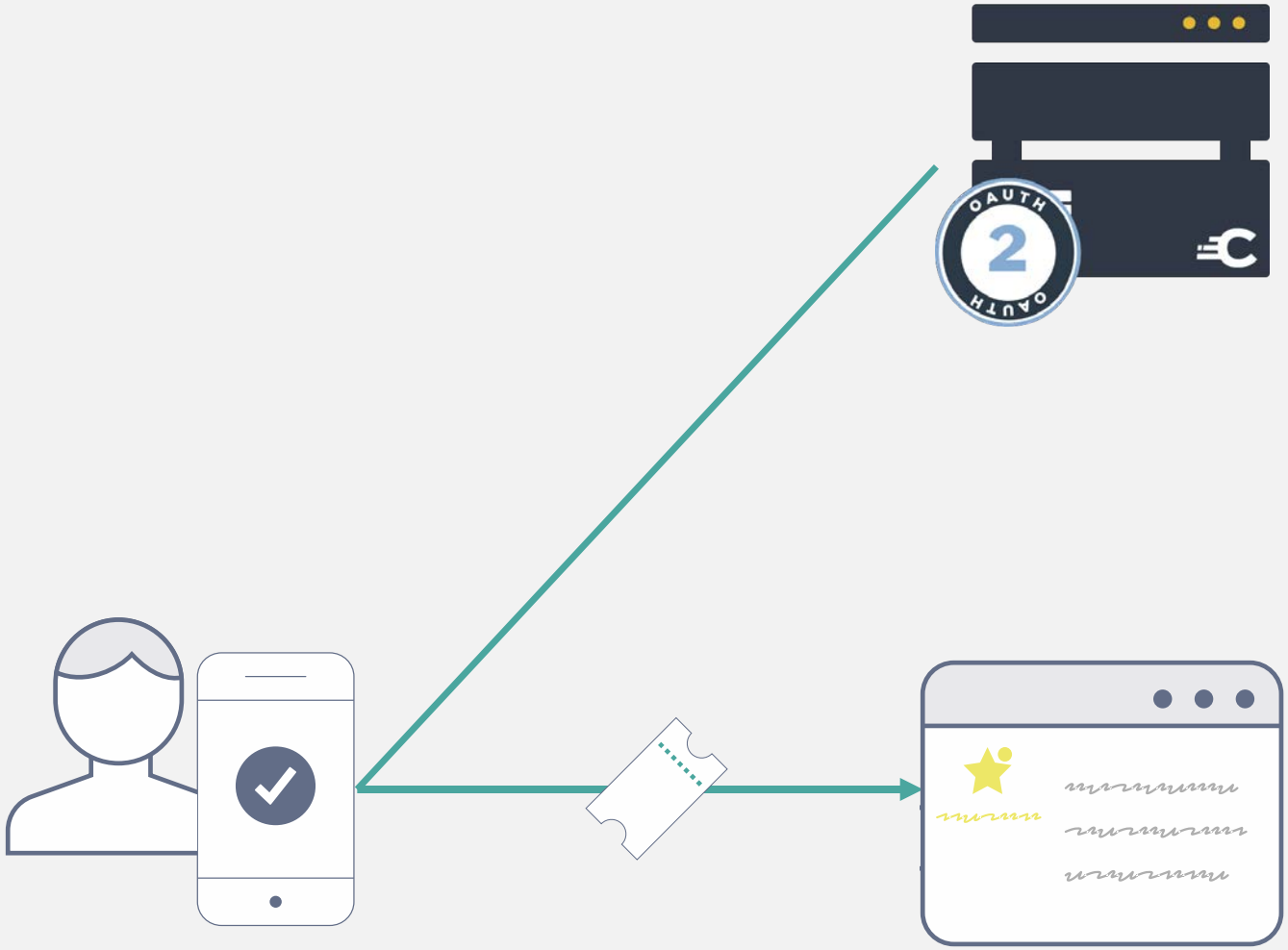


User logs in and delegates access

APIs & microservices

Copyright © 2018 Curity AB

Code Flow

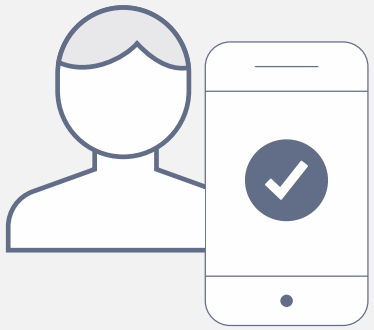


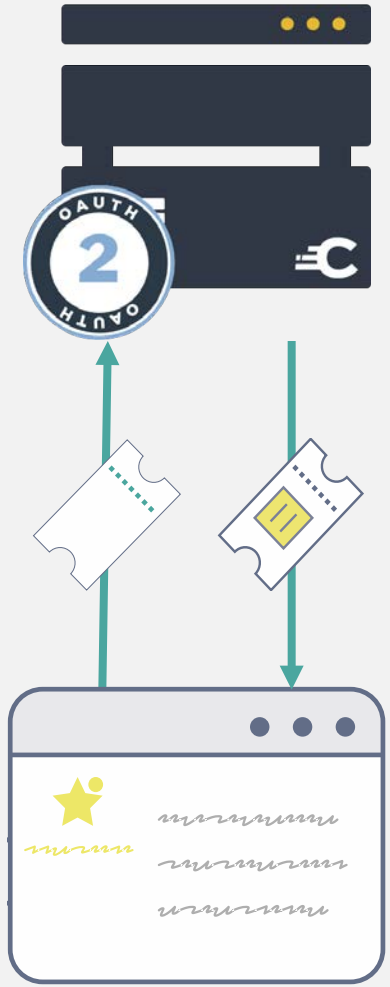
Short-lived access code is issued to client

APIs & microservices

Copyright © 2018 Curity AB

Code Flow





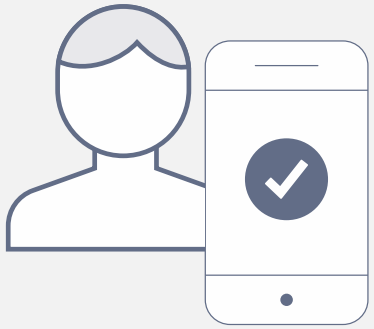
Code is exchanged for an access token

APIs & microservices

Copyright © 2018 Curity AB

Code Flow

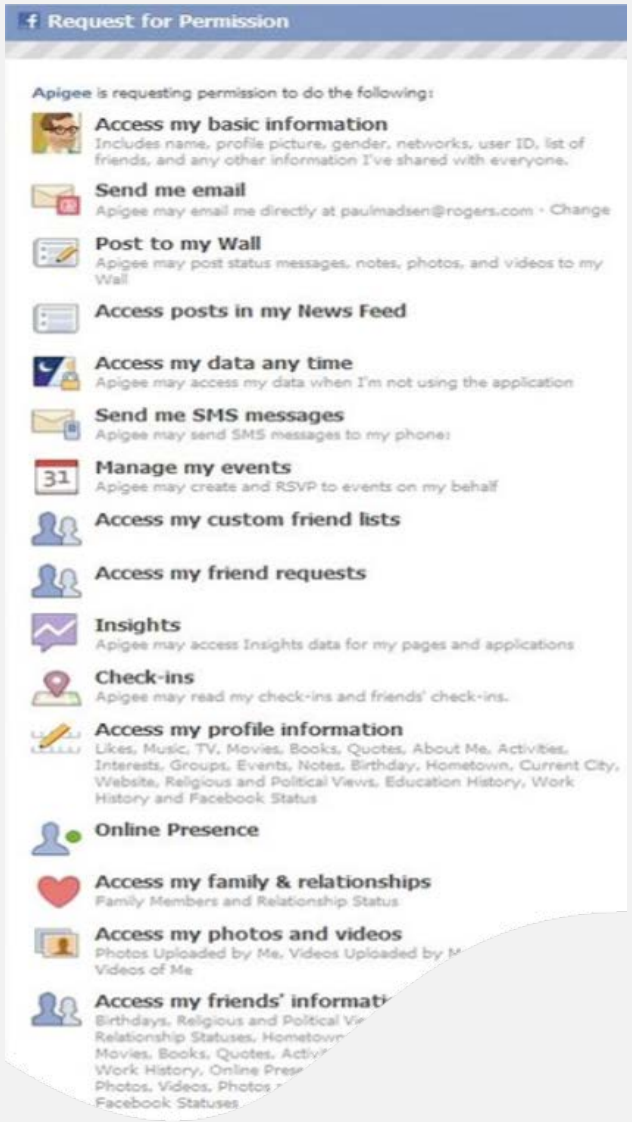
Access token can be used to call APIs



Copyright © 2018 Curity AB

Scopes

- Like permissions
- Scopes specify extent of tokens' usefulness
- Listed on consent UI (if shown)
- No standardized scopes



Copyright © 2018 Curity AB

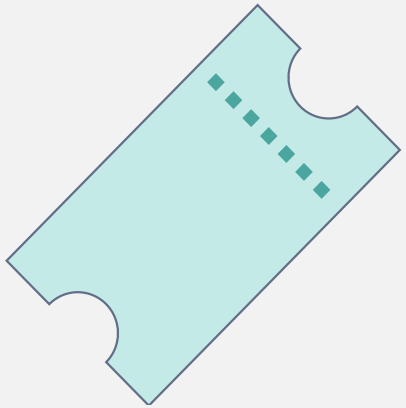
Kinds of Tokens

Access Tokens

Like a session

Used to secure API calls

Refresh Tokens



Like a Password

Used to get new access tokens

Copyright © 2018 Curity AB

Profiles of Tokens

Bearer

Bearer tokens are like cash

Holder of Key

HoK tokens are like credit cards

Copyright © 2018 Curity AB

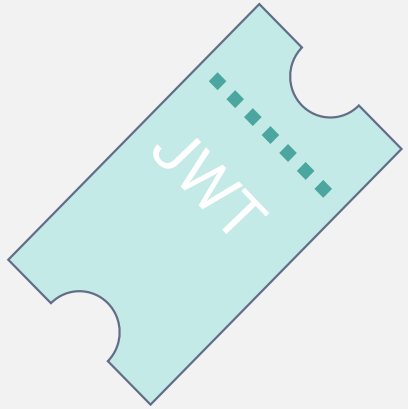
Types of Tokens

- WS-Security & SAML
- Custom
  - Home-grown
  - Oracle Access Manager
  - SiteMinder
- CBOR Web Tokens (CWT)
- JWT

Copyright © 2018 Curity AB

JWT Type Tokens

- Pronounced like the English word “jot”
- Lightweight tokens passed in HTTP headers & query strings
- Encoded as JSON
- Compact
- Encrypted, signed, or neither
- Not the only kind of token allowed by OAuth



Copyright © 2018 Curity AB

Passing Tokens

By Value

User attributes are in the token

By Reference

User attributes are referenced by an identifier

Copyright © 2018 Curity AB

Improper Usage of OAuth

Not for authentication

Not for federation

Not *really* for authorization

Copyright © 2018 Curity AB

Proper Usage or OAuth

For delegation

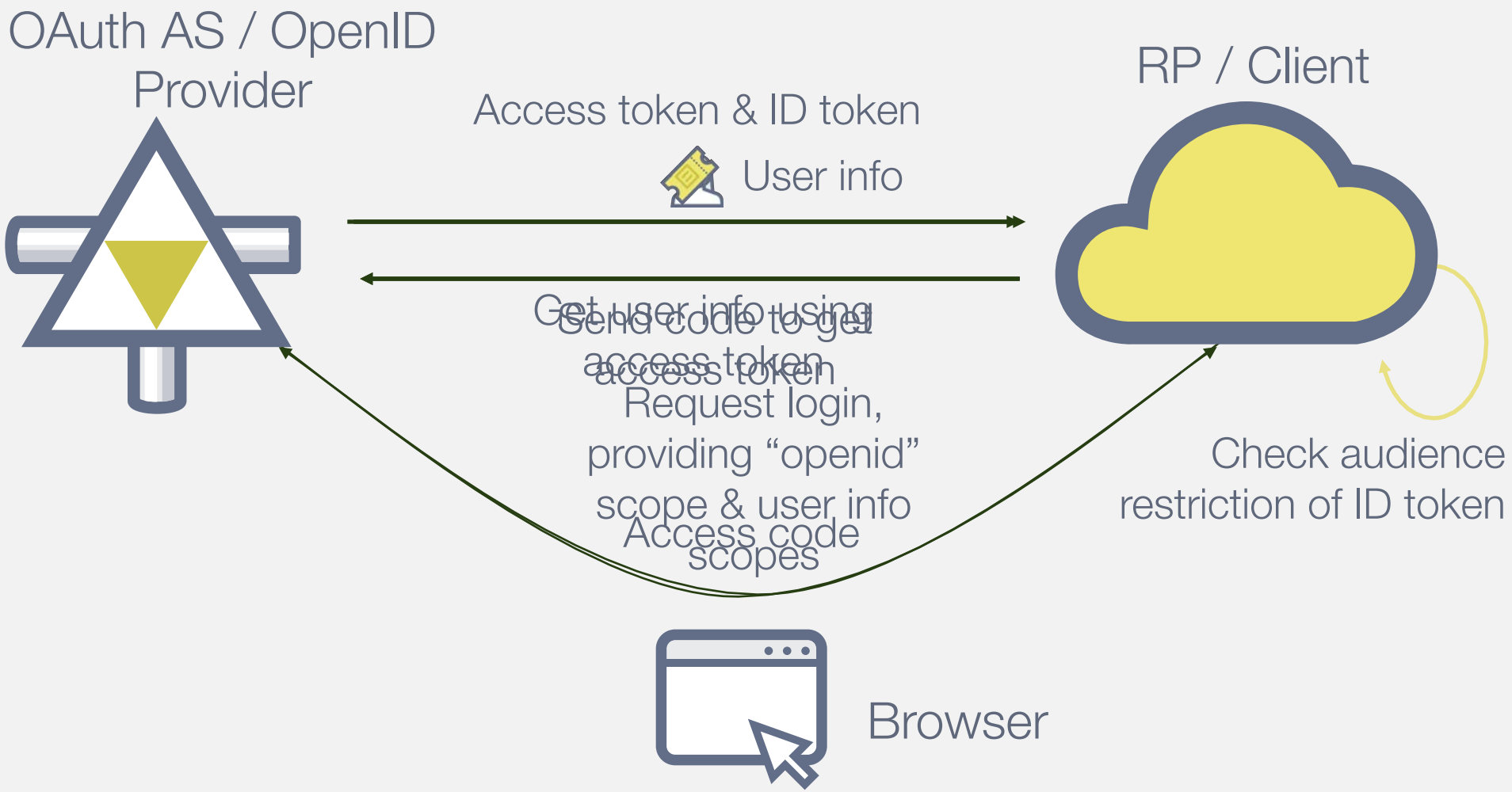
Copyright © 2018 Curity AB

OpenID Connect

- Next generation federation protocol
  - Based on OAuth 2
  - Made for mobile
  - Not backward compatible
- Client & API receive tokens
- User info endpoint provided for client to get user data

Copyright © 2018 Curity AB

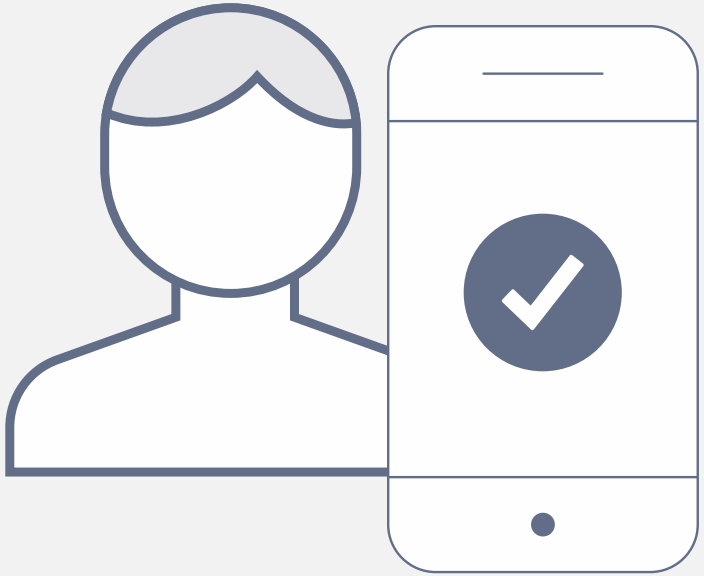
OpenID Connect Examples



Copyright © 2018 Curity AB

ID Token is for the Client

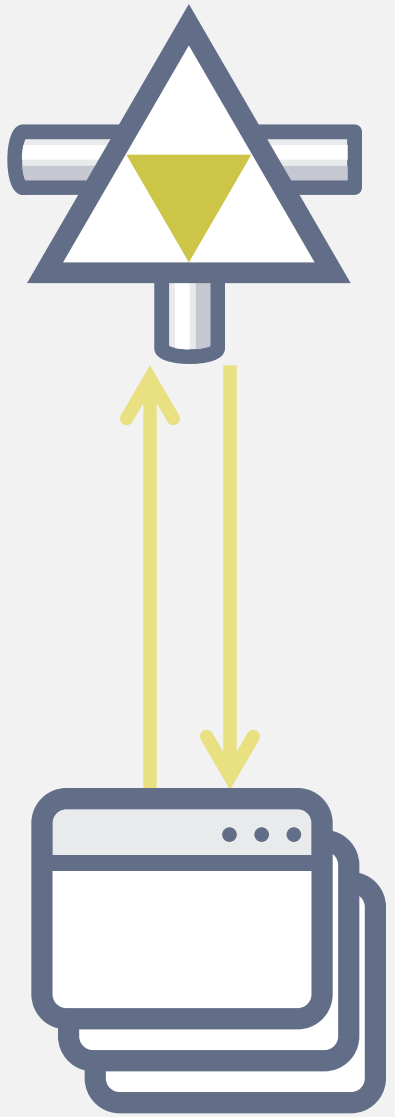
- Access token is for API
- ID token is for client
- ID token provides client with info about
  - Intended client recipient
  - Username
  - Credential used to login
  - Issuer of token
  - Expiration time



Copyright © 2018 Curity AB

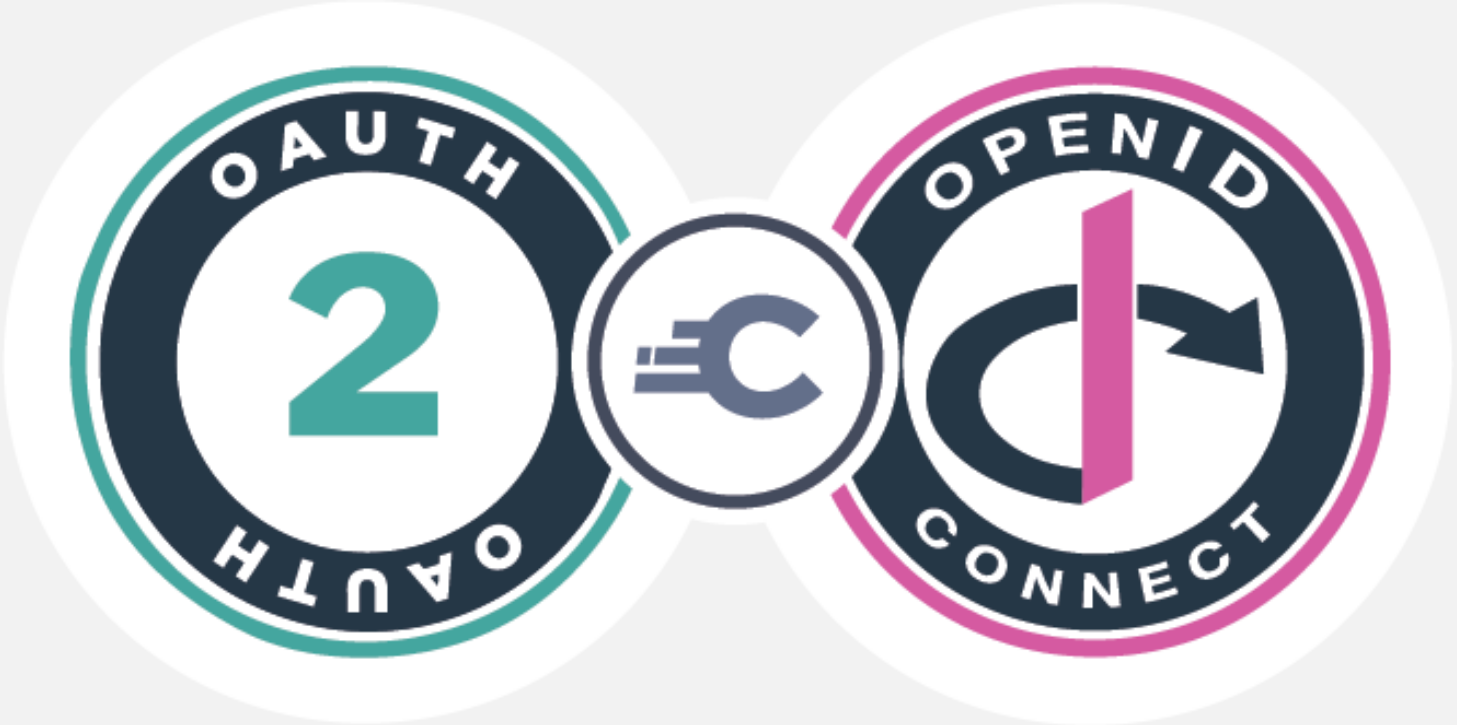
User Info Endpoint

- Token issuance and user discovery endpoint
- Authenticate using access token issued by OpenID Provider
- Output depends on requested and authorized scopes
- sub claim must match sub claim in ID token



Copyright © 2018 Curity AB

Applied to Microservices and APIs

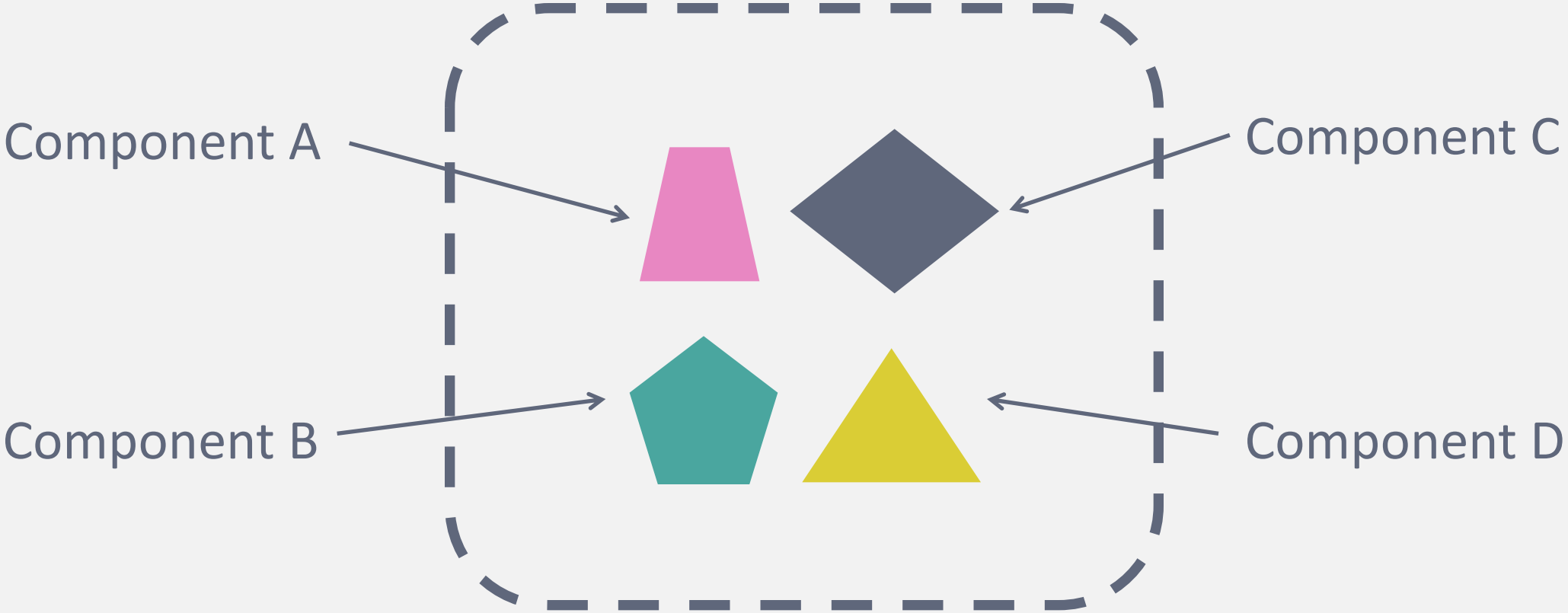


Copyright © 2018

A Traditional Service

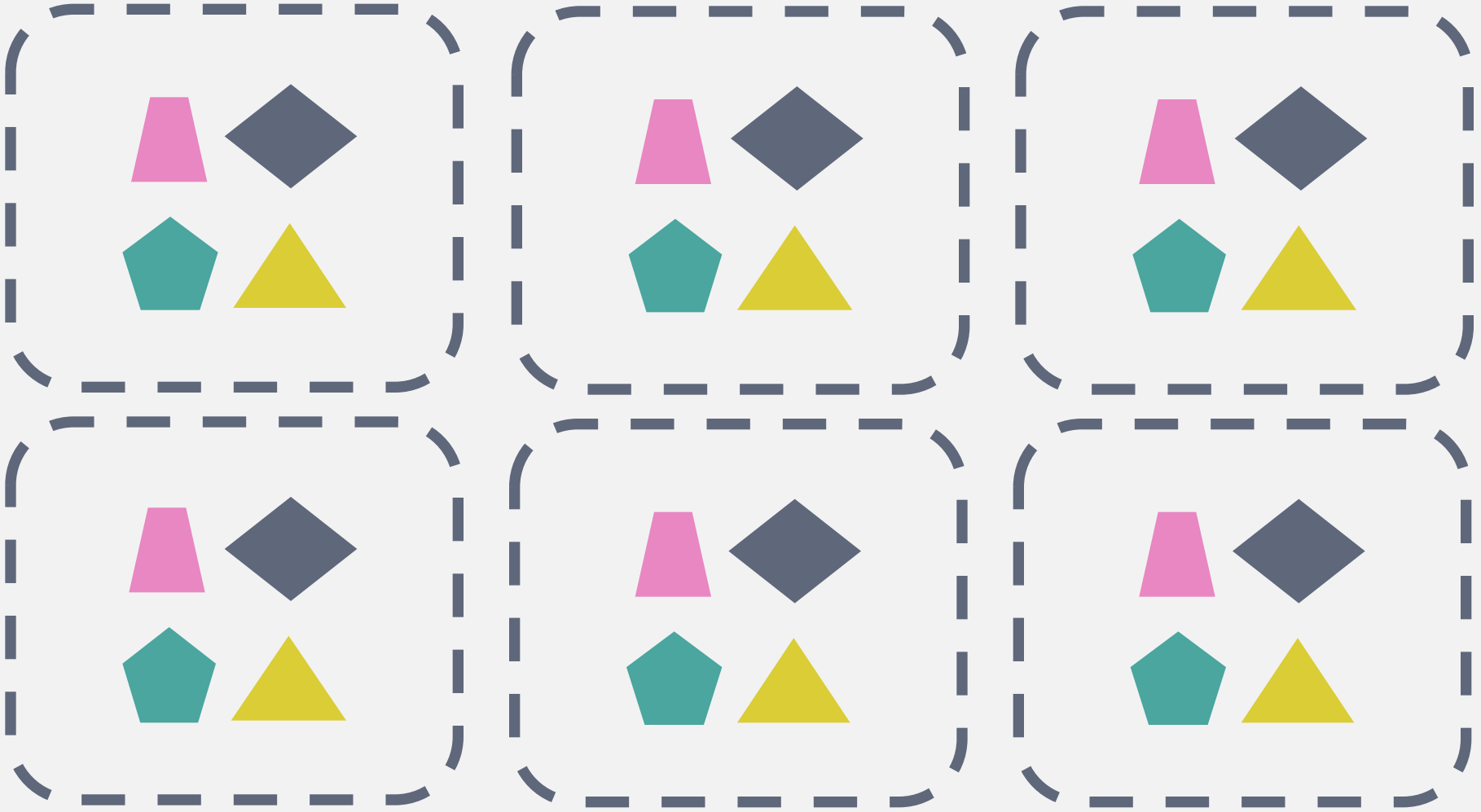
Copyright © 2018 Curity AB

With Traditional Subsystems



Copyright © 2018 Curity AB

… and traditional scalability



Copyright © 2018 Curity AB

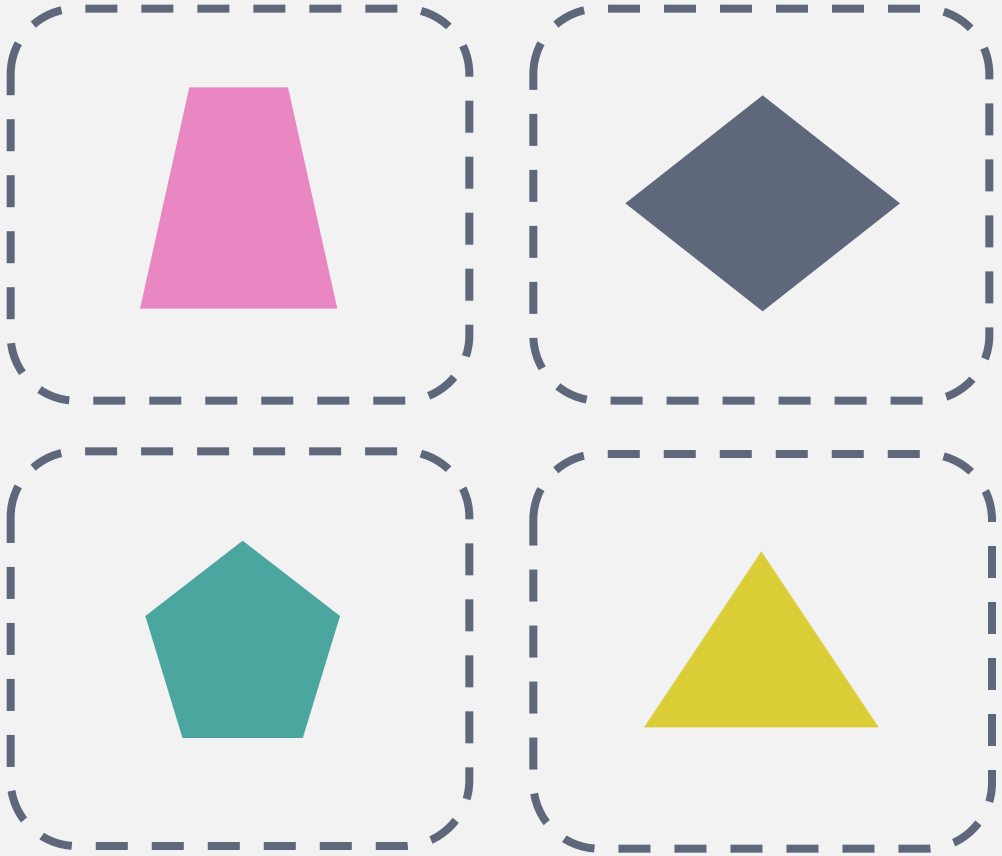
But this is not always how we build systems

Copyright © 2018 Curity AB

One Microservice

Copyright © 2018 Curity AB

Many Microservices

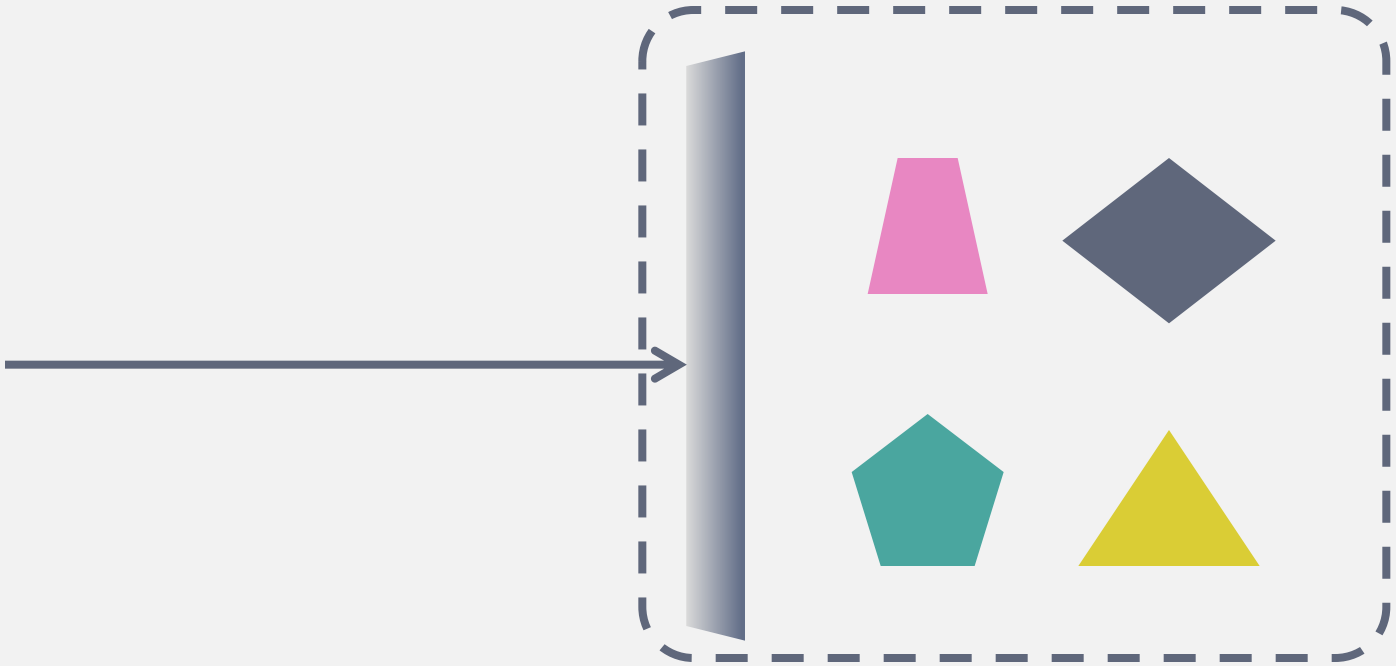


Copyright © 2018 Curity AB

Scaling Microservices

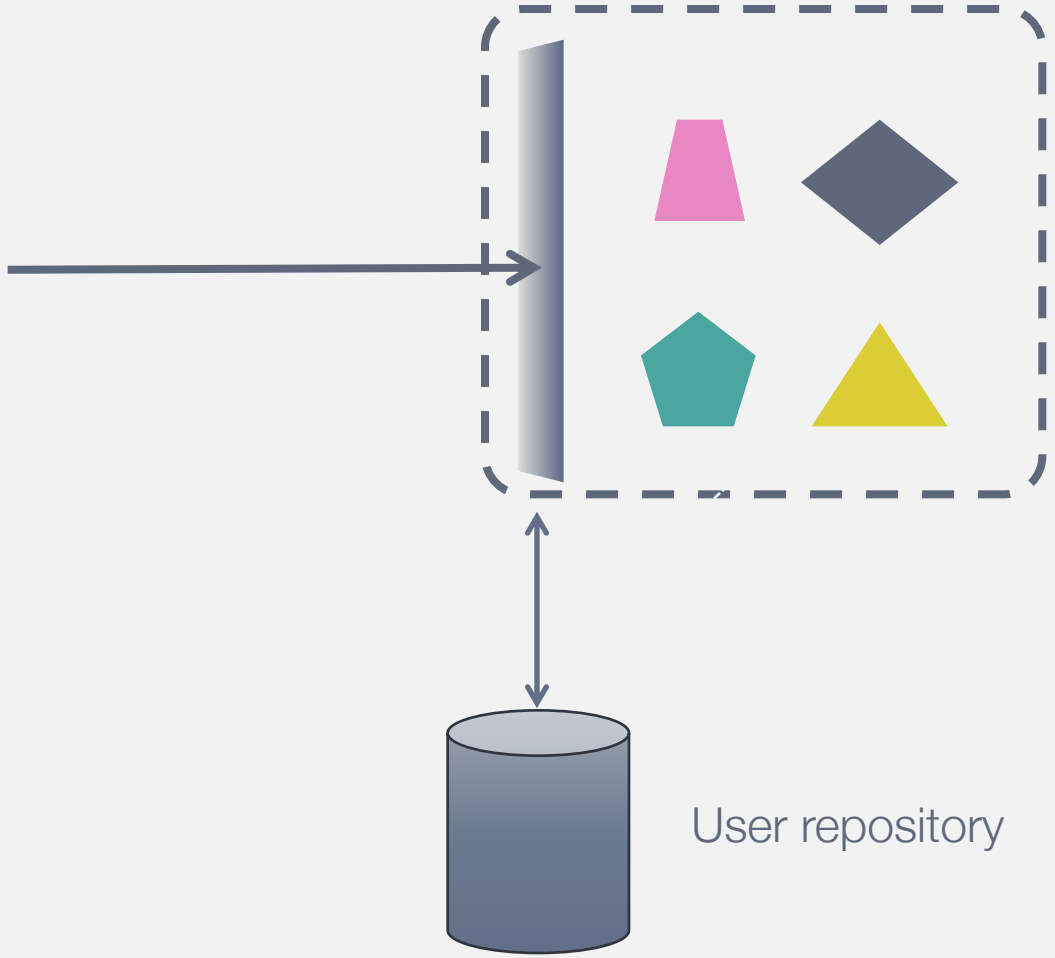
Copyright © 2018 Curity AB

Securing Traditional Services



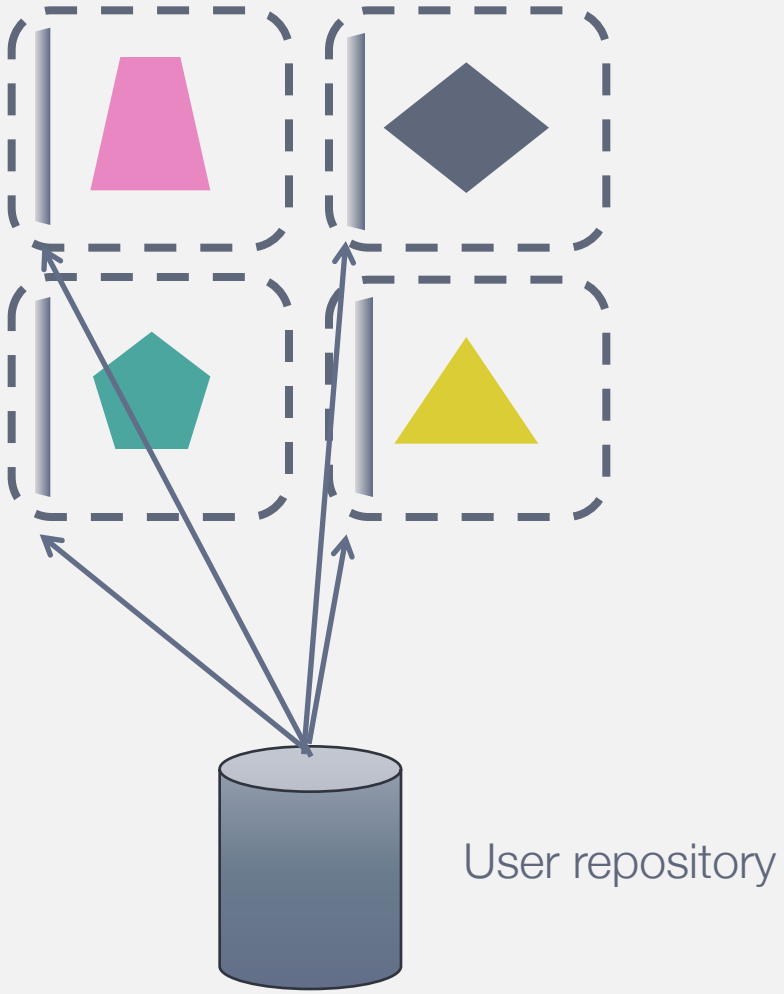
Copyright © 2018 Curity AB

Securing Traditional Services



Copyright © 2018 Curity AB

So for microservices that would mean…



Copyright © 2018 Curity AB

Remember our two token passing methods?

By Value

User attributes are in the token

By Reference

User attributes are referenced by an identifier

Copyright © 2018 Curity AB

By Reference

Contains NO information outside the network

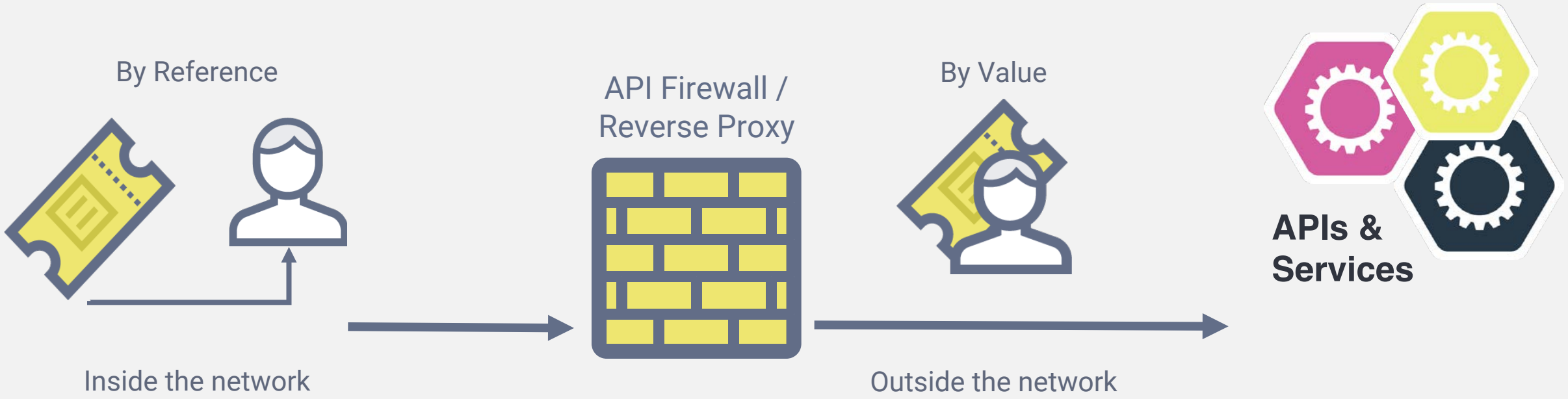
Copyright © 2018 Curity AB

By Value

Contains ALL *necessary* information

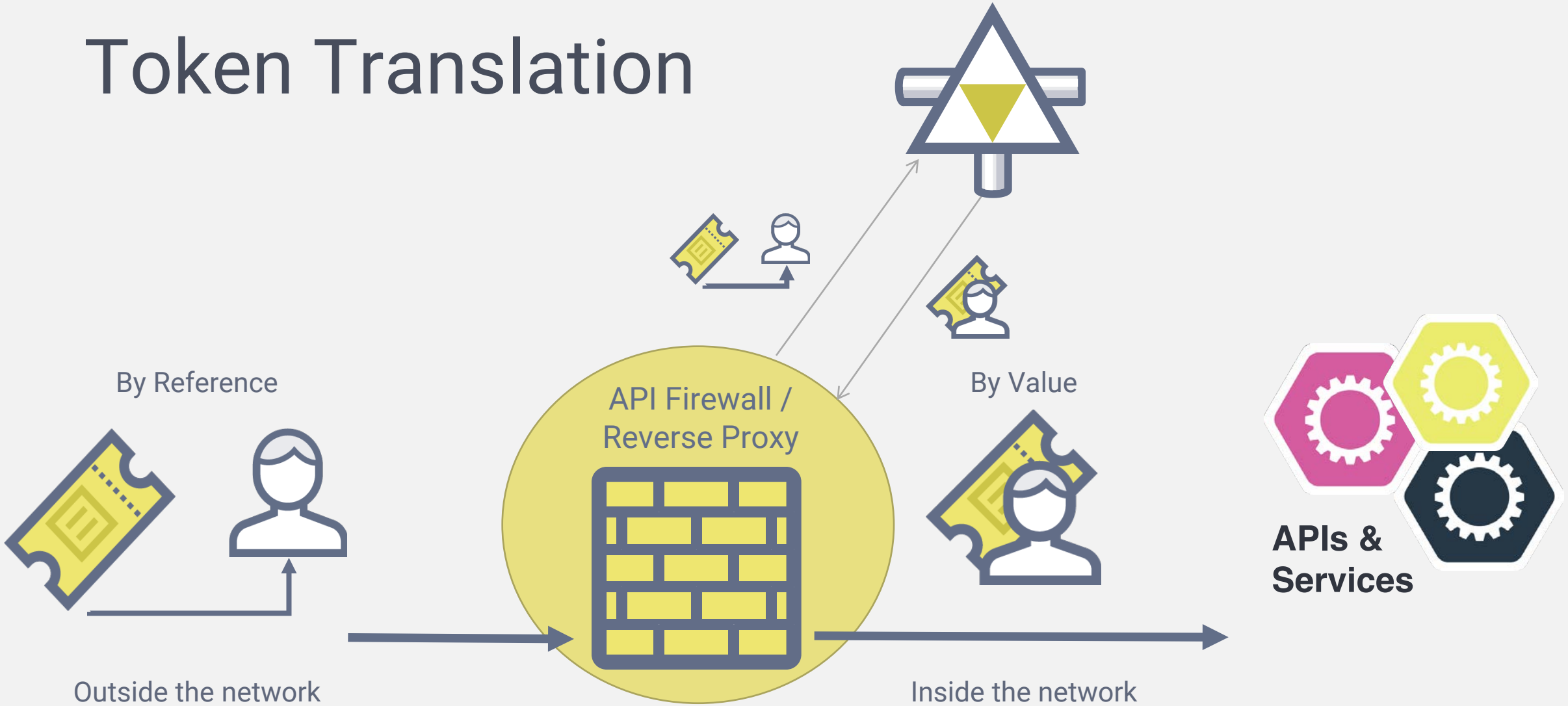
Copyright © 2018 Curity AB

External vs. Internal



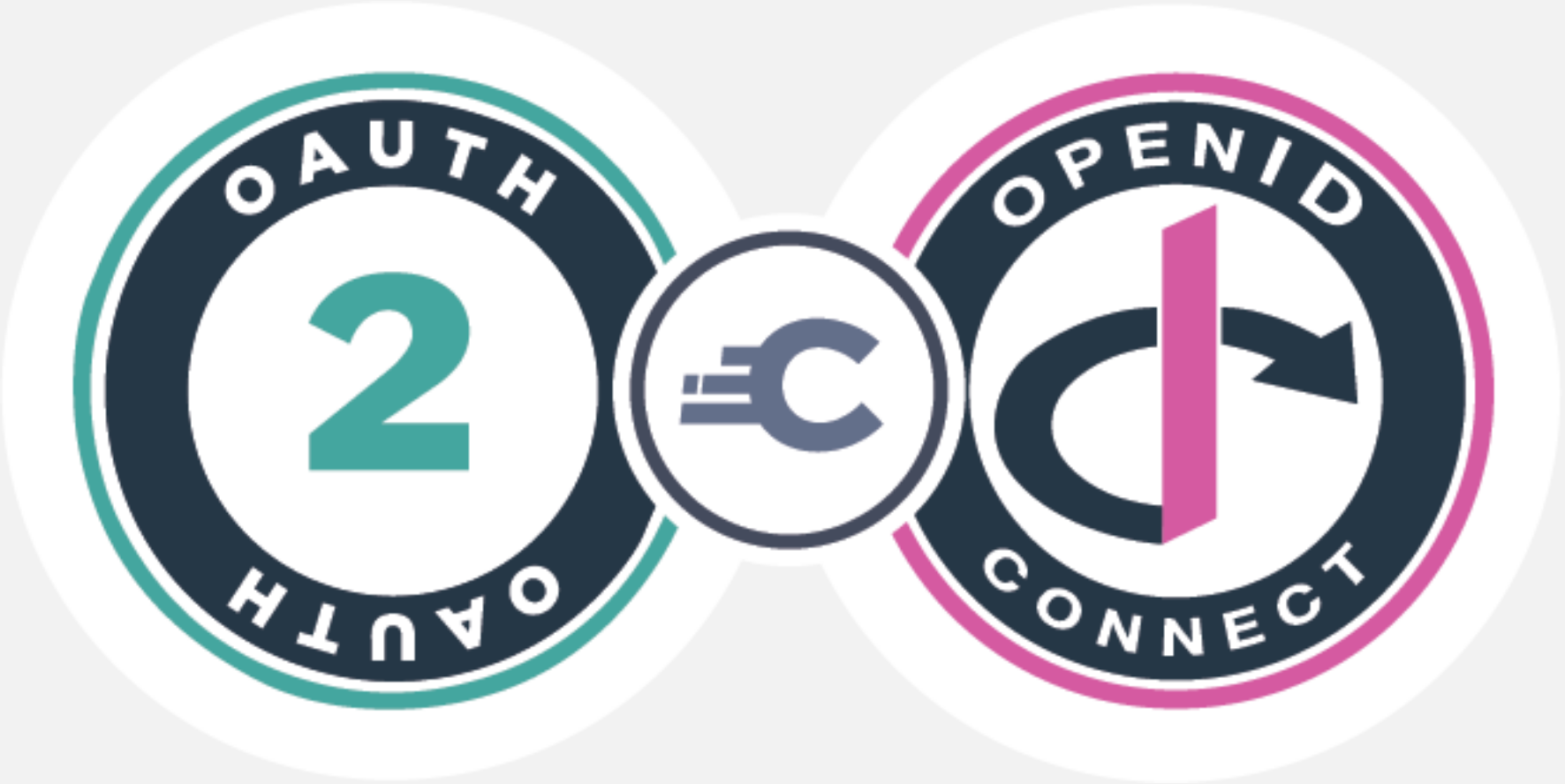
Copyright © 2018 Curity AB

Token Translation



Copyright © 2018 Curity AB

Demo



Copyright © 2018 Curity AB

Additional Resources

- Blog posts
  - bit.ly/oauth-deep-dive
  - bit.ly/4-api-security-defenses
  - bit.ly/building-secure-api
  - bit.ly/right-api-armor
  - https://bit.ly/2qn8Jj4

- Videos

  bit.ly/oauth-in-depth

  bit.ly/micro-services-security

  bit.ly/building-secure-api-video
- Whitepaper at our booth
- https://nordicapis.com/api-insights/security/

Copyright © 2018 Curity AB

Summary

- API security > API keys & OAuth
- OAuth 2 fundamentals
  - Token types
  - Profiles
  - Passing tokens
- Building OpenID Connect on OAuth
- Using those with microservices & for user-based delegation

Copyright © 2018 Curity AB

Visit curity.io and stop by our booth

Copyright © 2018 Curity AB