Service Principals, App Registrations and other Azure Myths

Eric Berg
www.ericberg.de
🐦 @ericberg_de

Eric Berg

- Vice President Consulting Expert @ CGI
- MVP Azure & CDM, LinkedIn Learning Trainer
- Cloud, Datacenter & Management
- info@ericberg.de
- @ericberg_de | @GeekZeugs
- www.ericberg.de | www.geekzeugs.de

Live

MOUNTAIN IT
www.ericberg.de

MVP Microsoft® Most Valuable Professional

GEEKZEUGS HOME OF
GEEKSPRECH Podcast
GEEKSCHAU Webcast
GEEKTREFF Community

Azure Meetup THÜRINGEN

User Assigned

App Registration

Service Connections

Client ID

Service Principal

Enterprise App

App Consent

Managed Identity

Security Principal

Client Secret

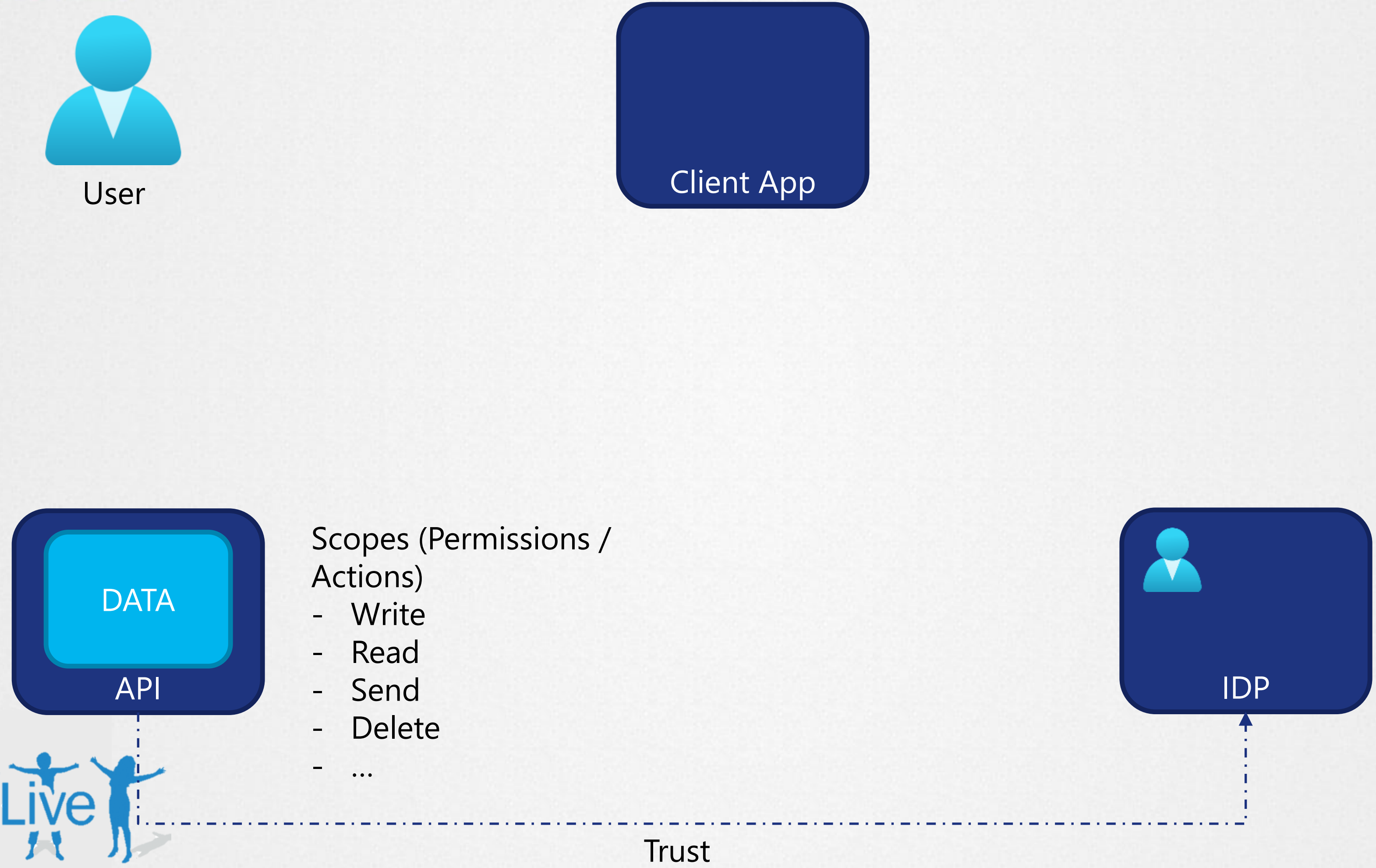
System Assigned

User Principal

Application Object

...

What is it all about?



User

Client App

DATA

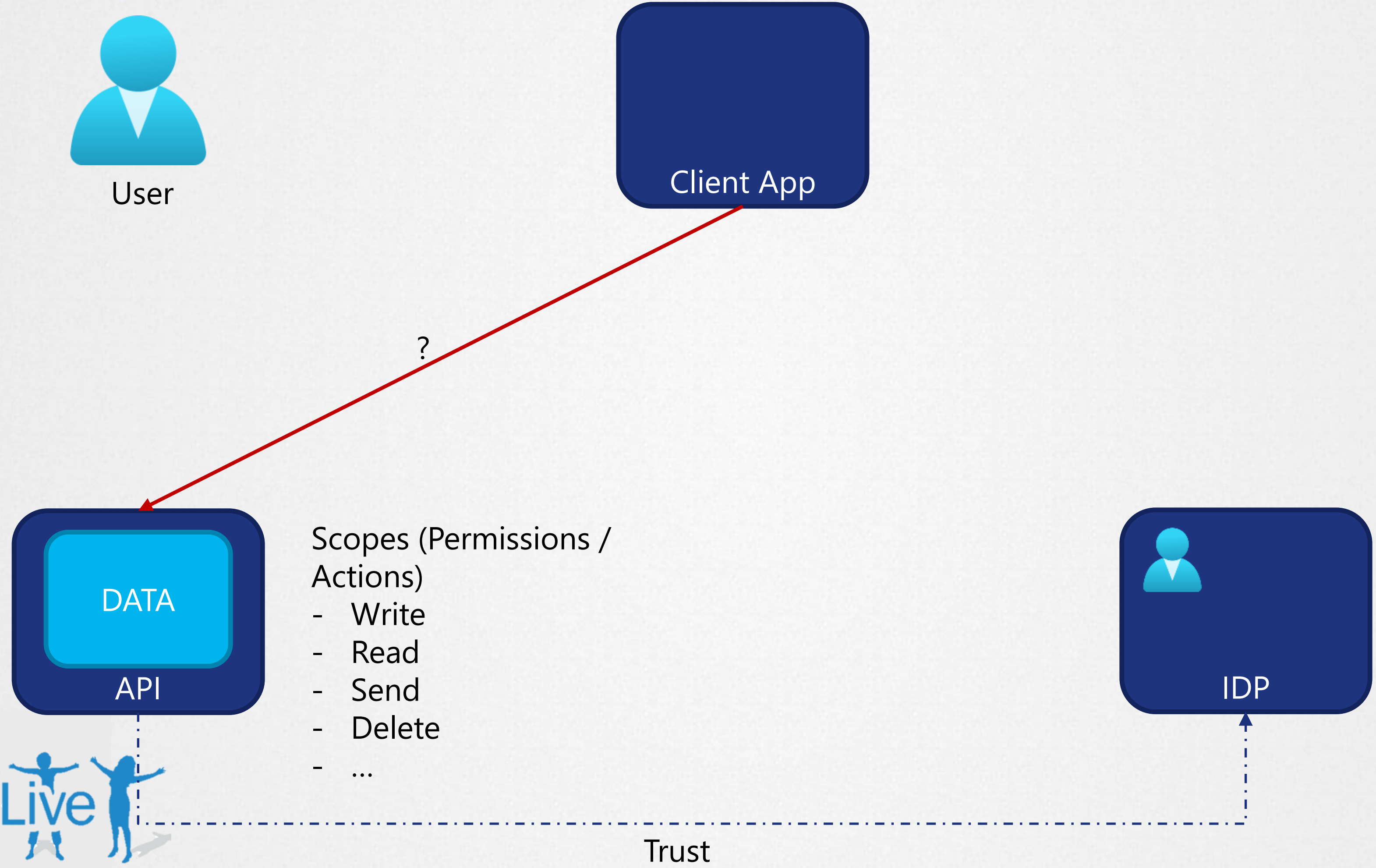
API

IDP

Trust

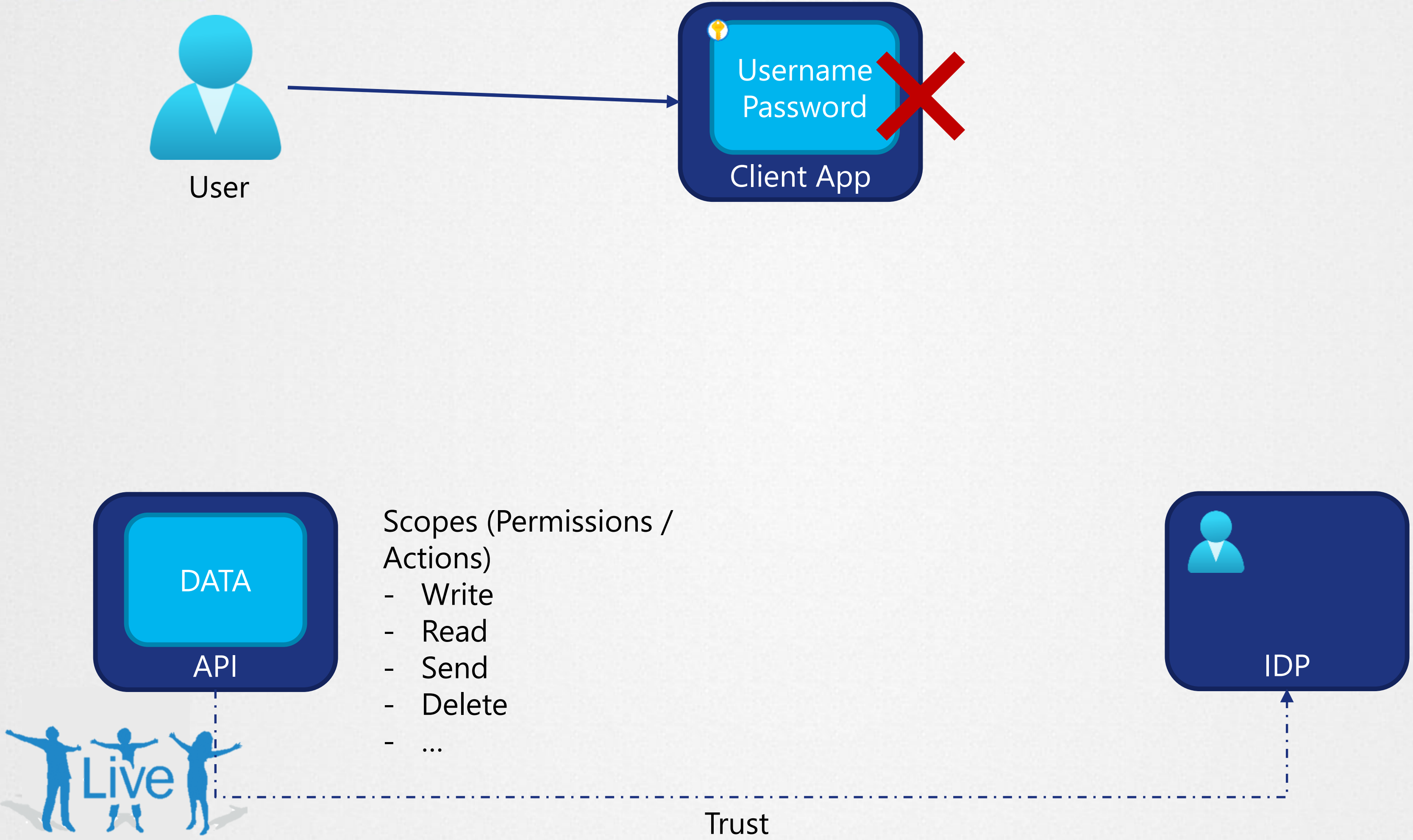
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...



Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...



User

Username
Password

Client App

DATA

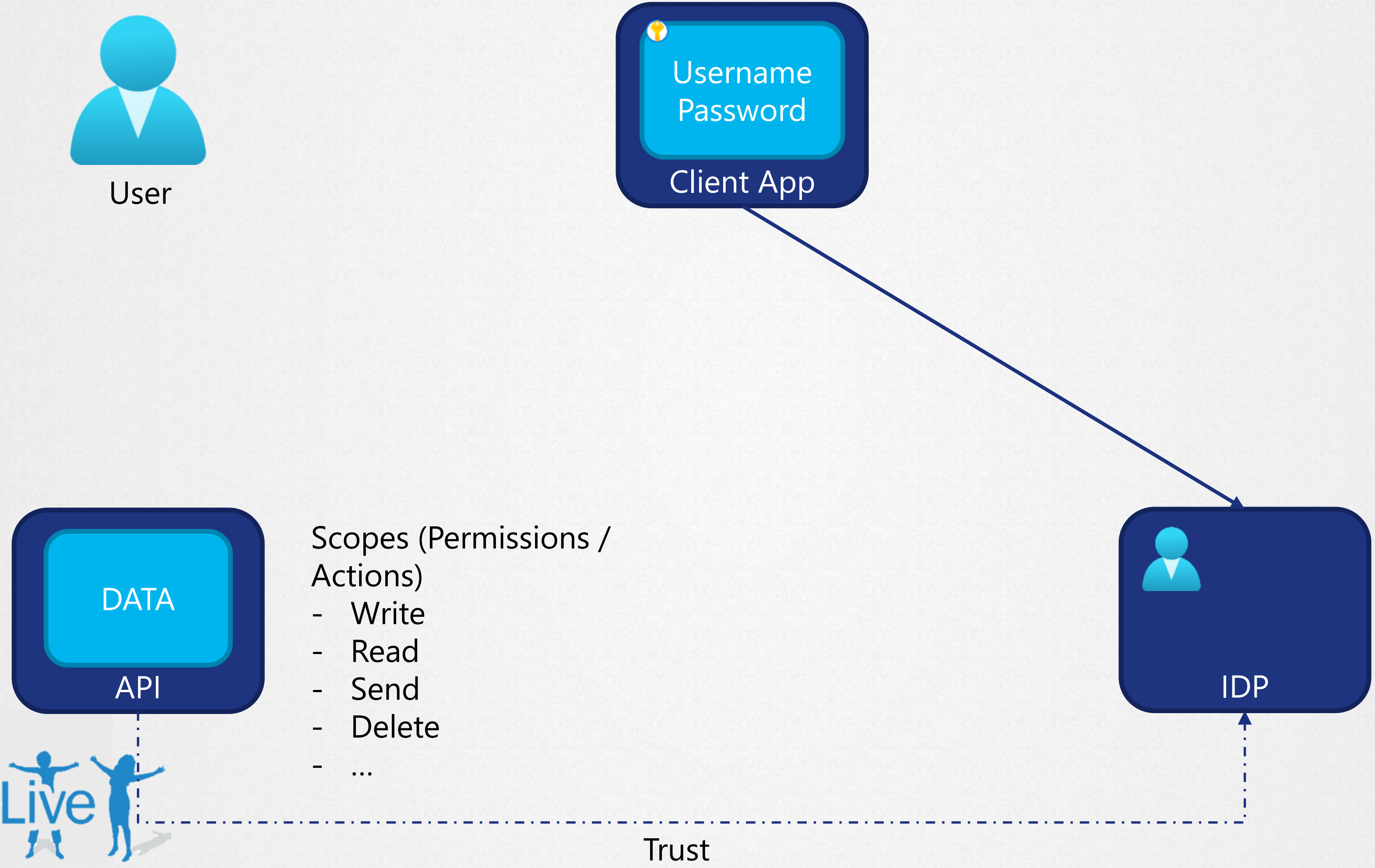
API

Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

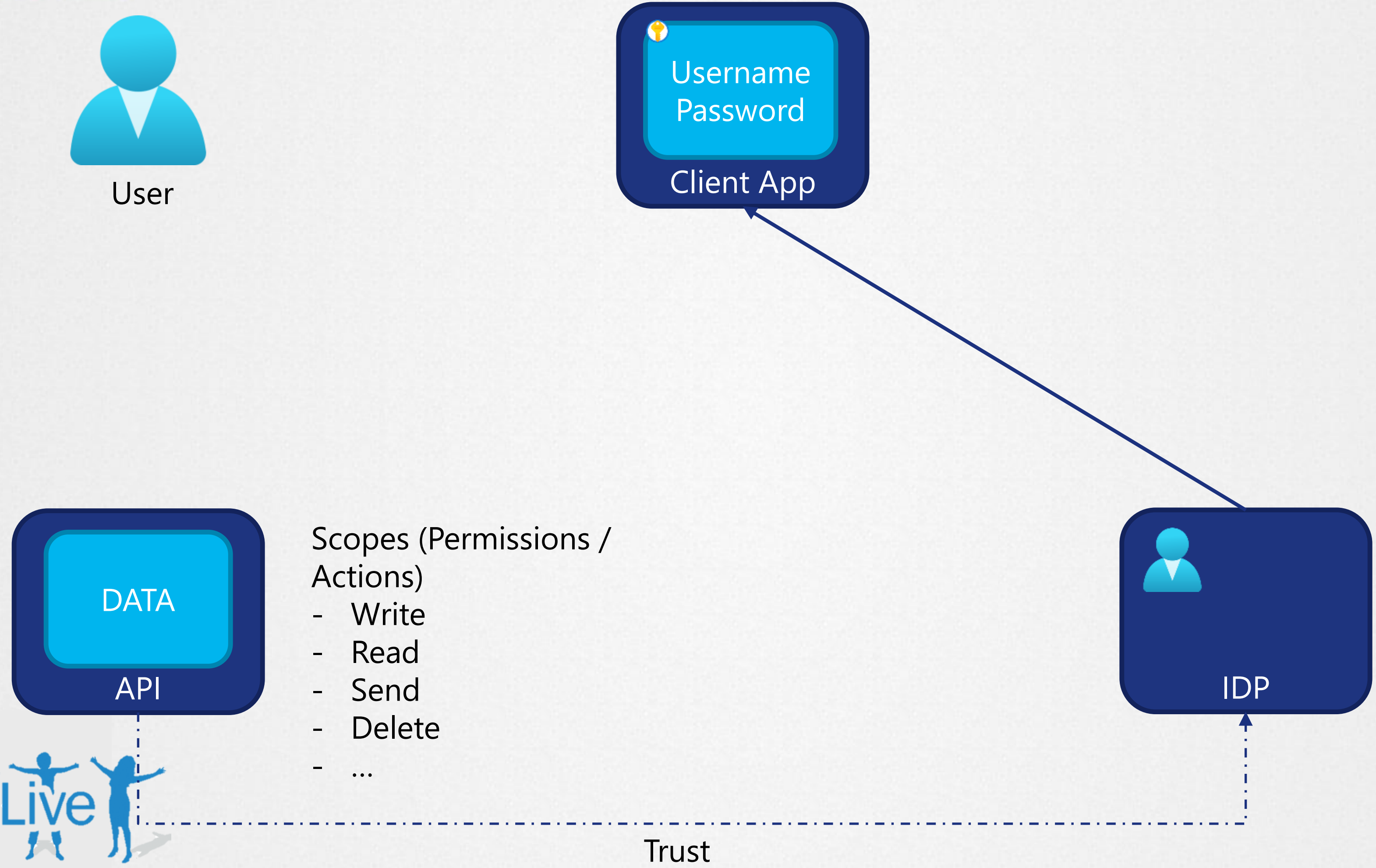
IDP

Trust



Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...



User

Username
Password

Client App

DATA

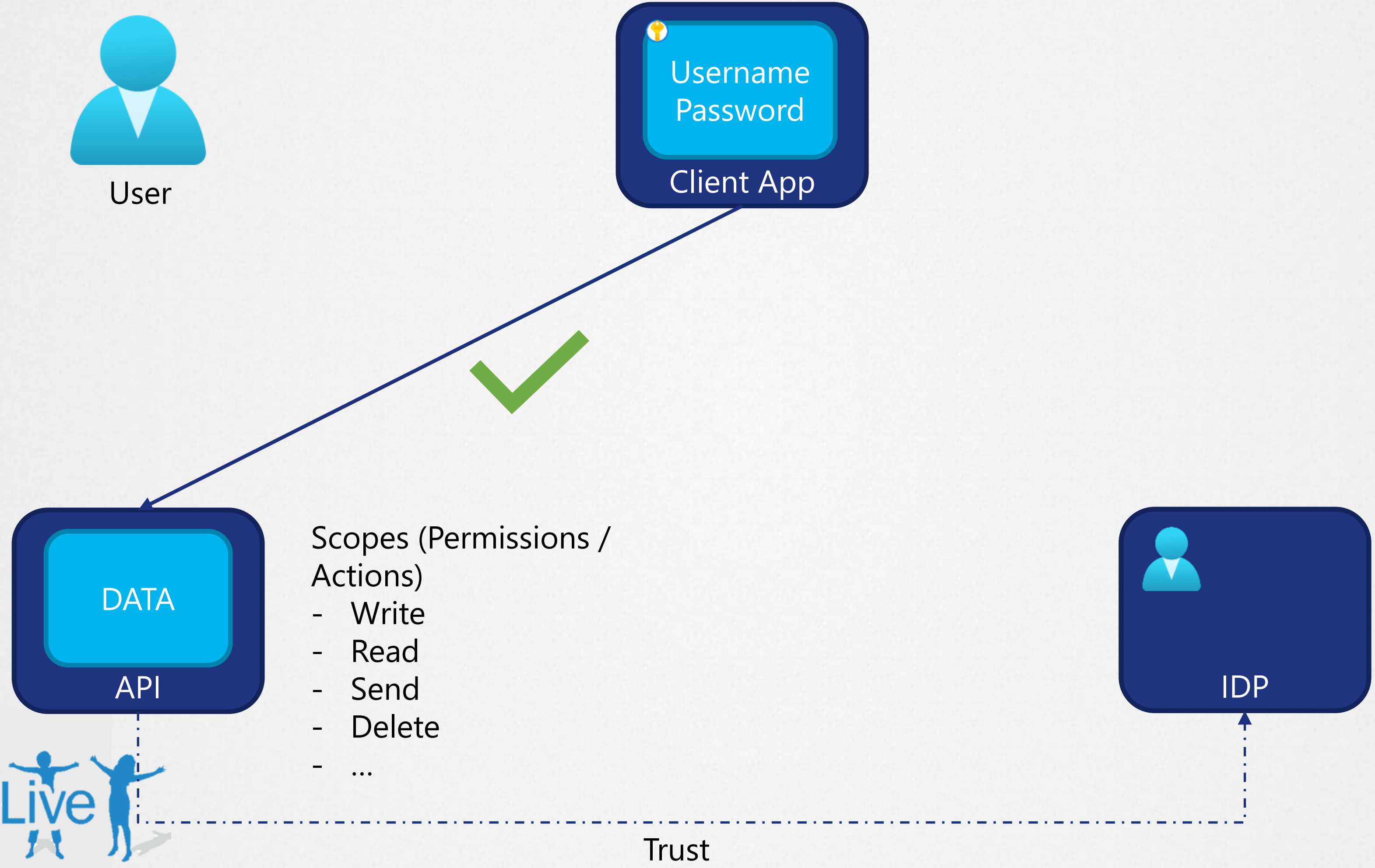
API

IDP

Trust

Scopes (Permissions / Actions)

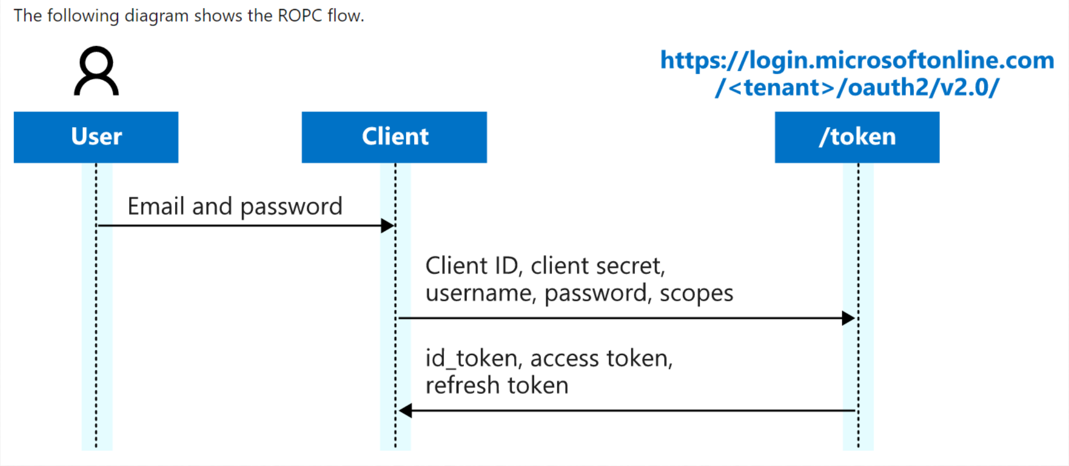
- Write
- Read
- Send
- Delete
- …



Scopes (Permissions / Actions)

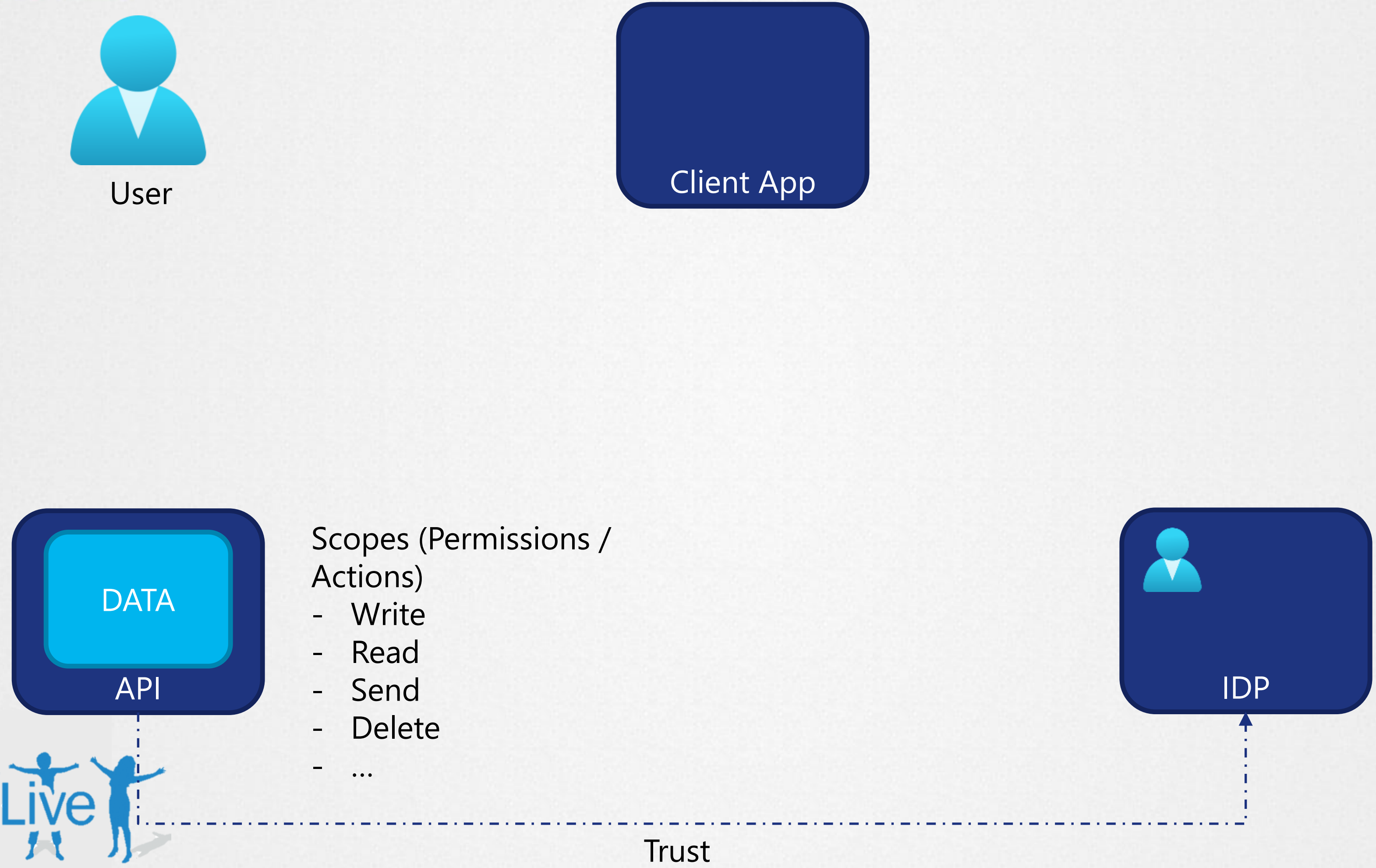
- Write
- Read
- Send
- Delete
- …

This is how it flows … in AAD



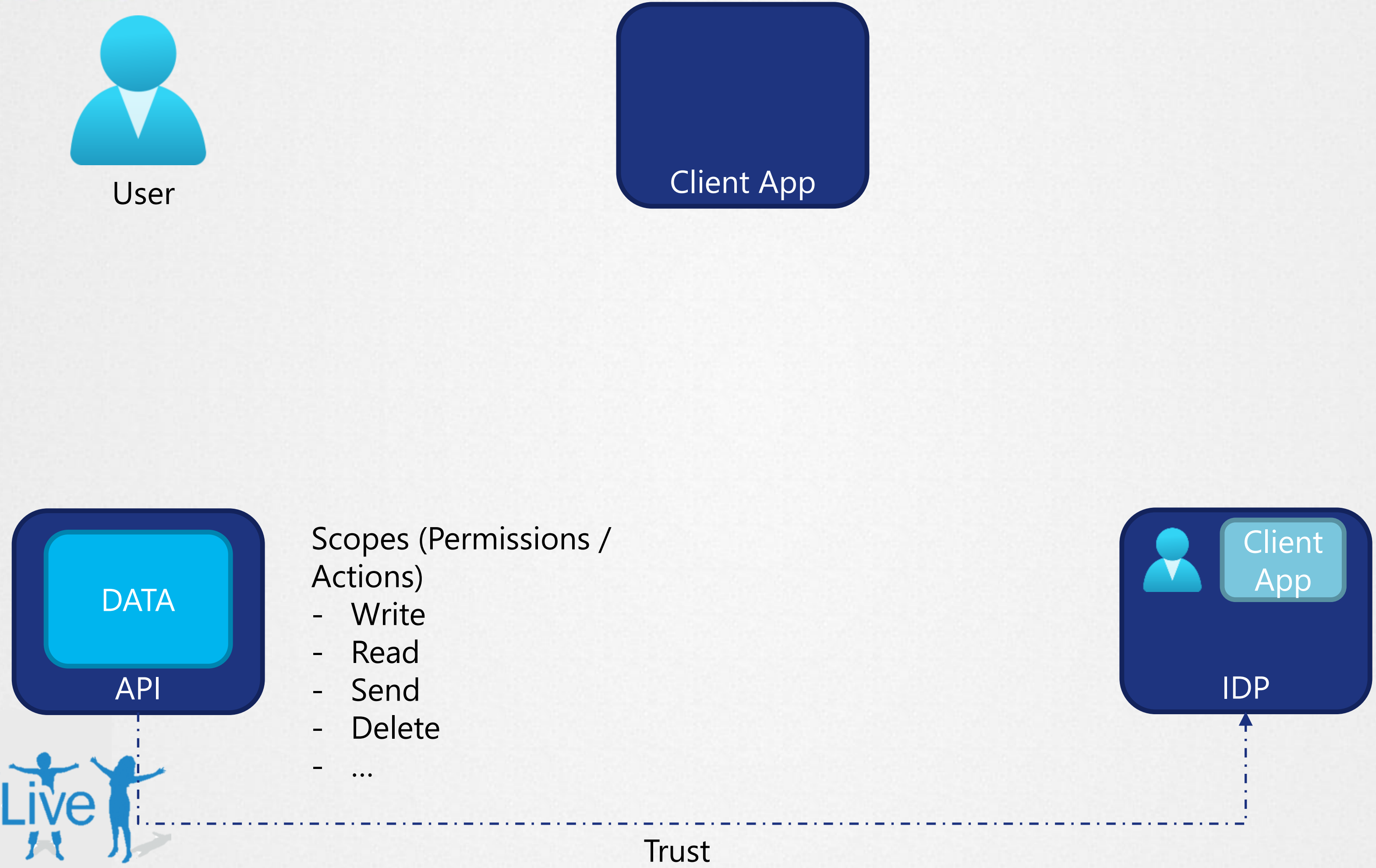
The following diagram shows the ROPC flow.

How to do it better?



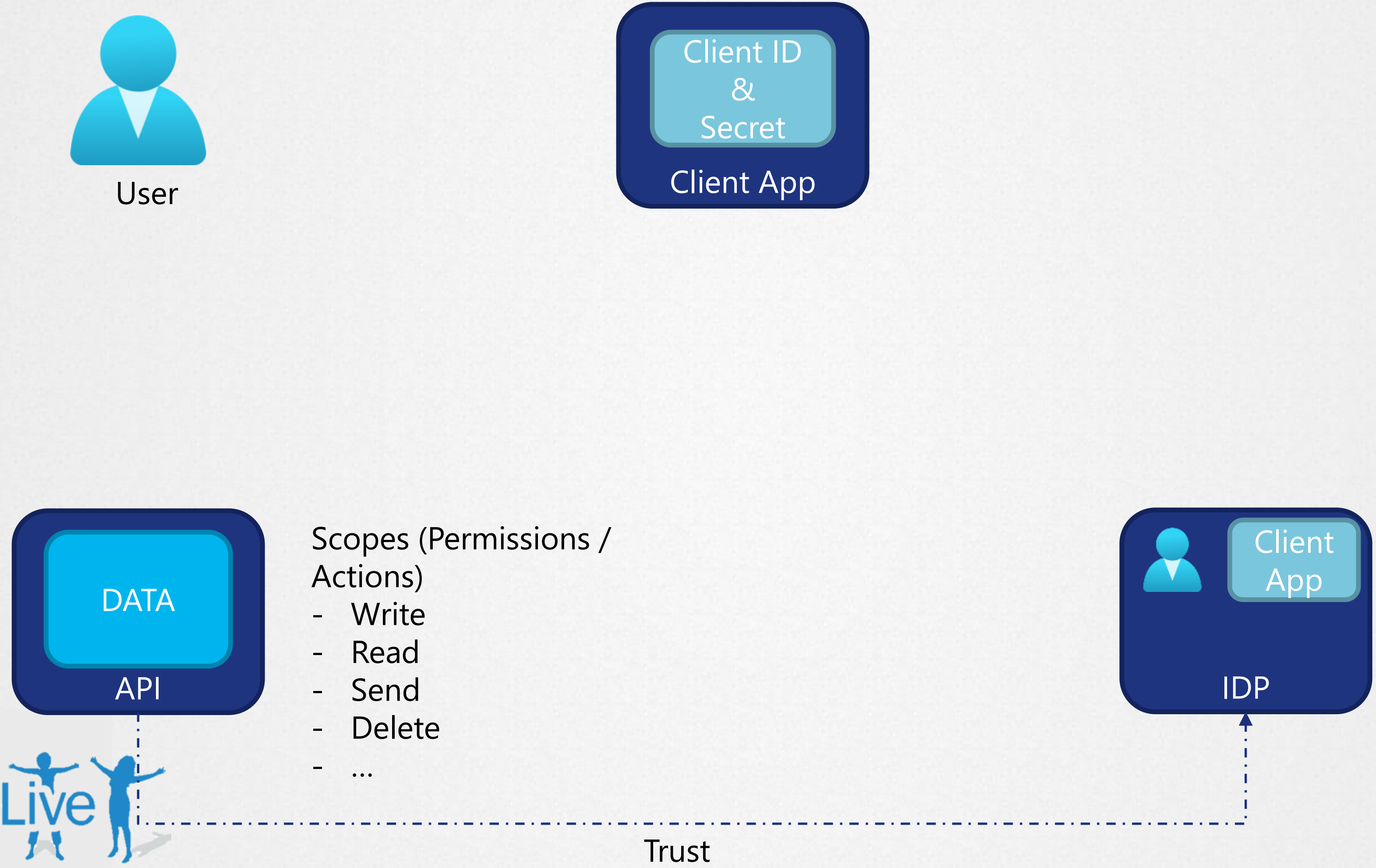
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …



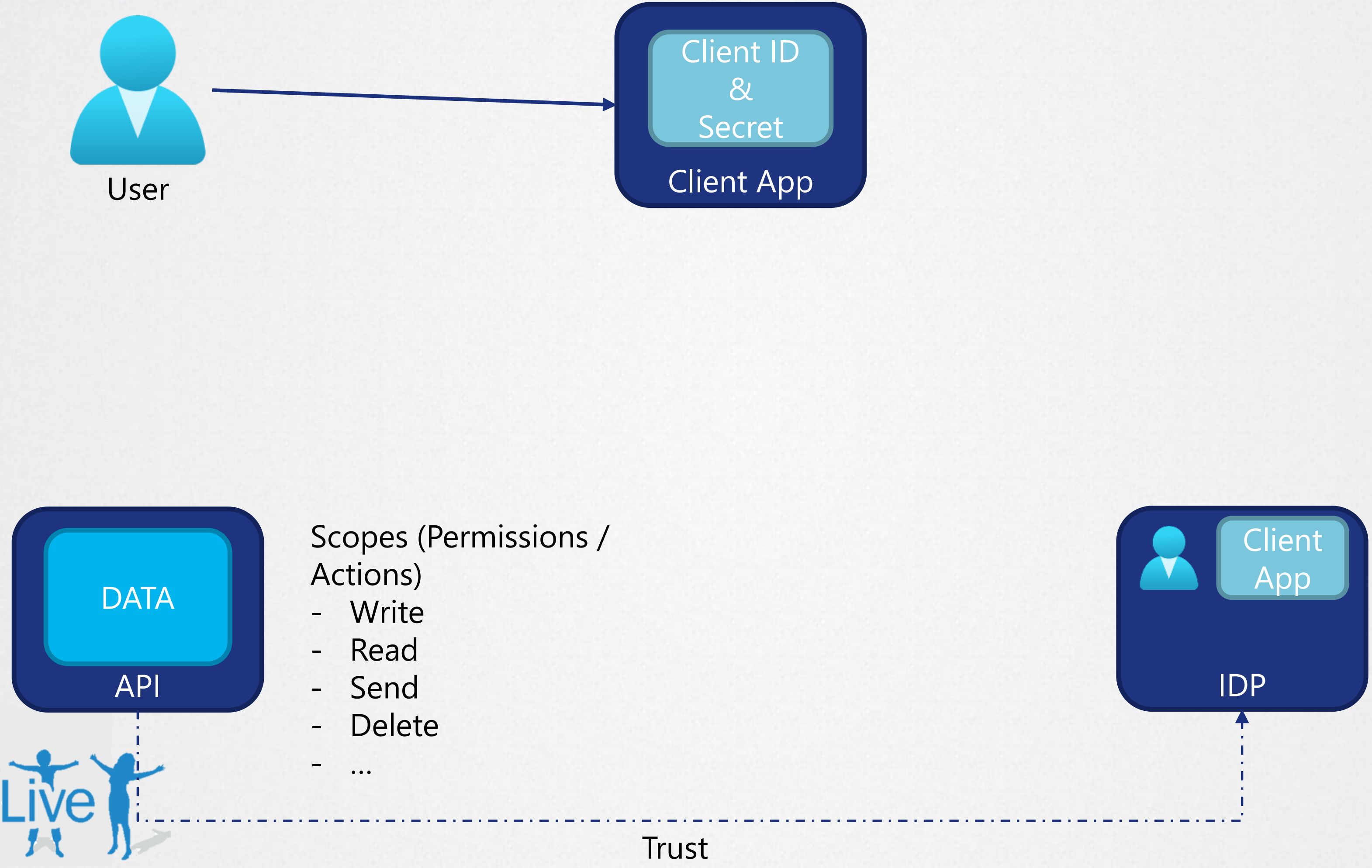
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …



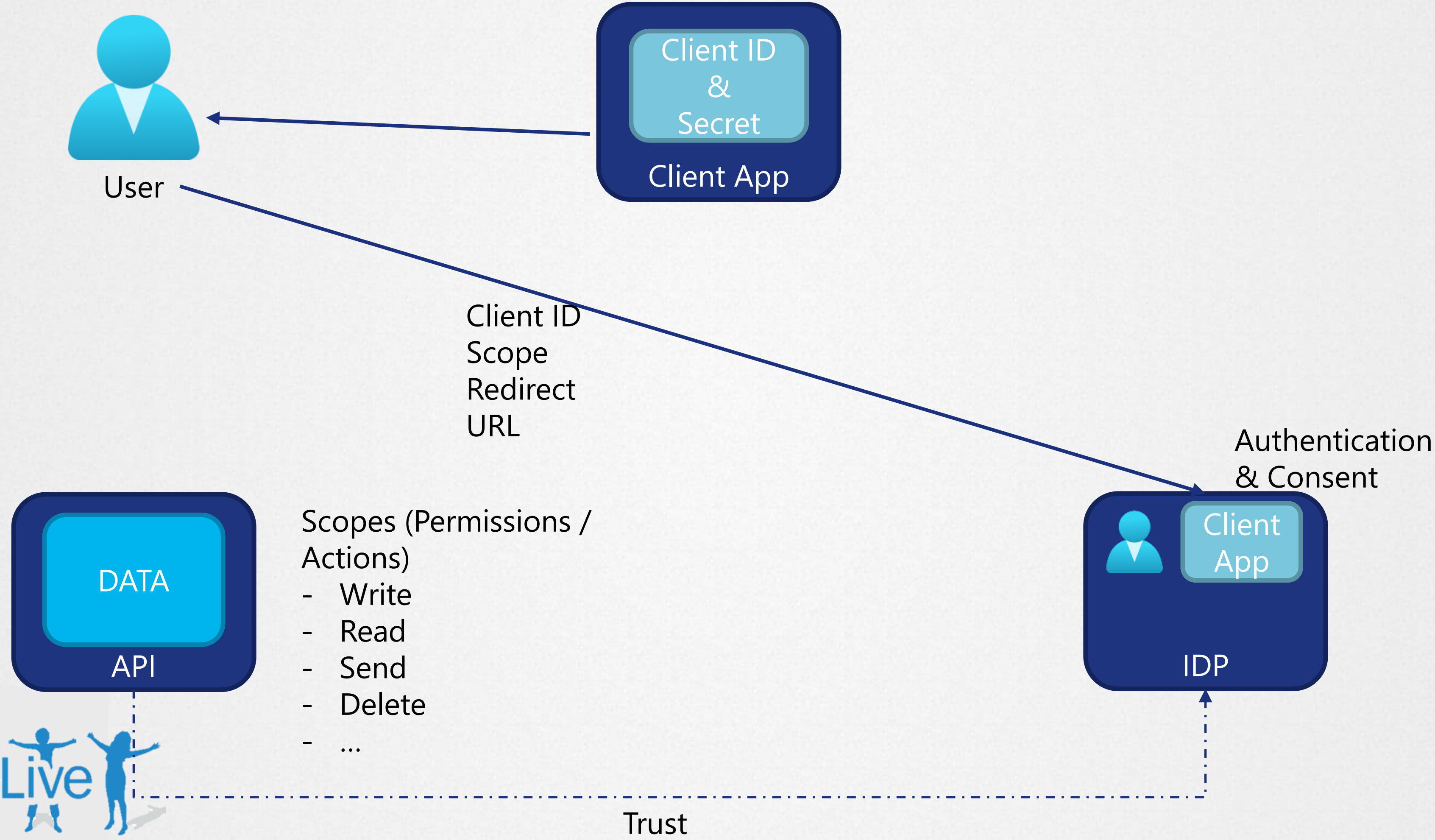
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...



Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...



User

Client ID
&
Secret

Client App

Client ID
Scope
Redirect
URL

Authentication
& Consent

DATA

API

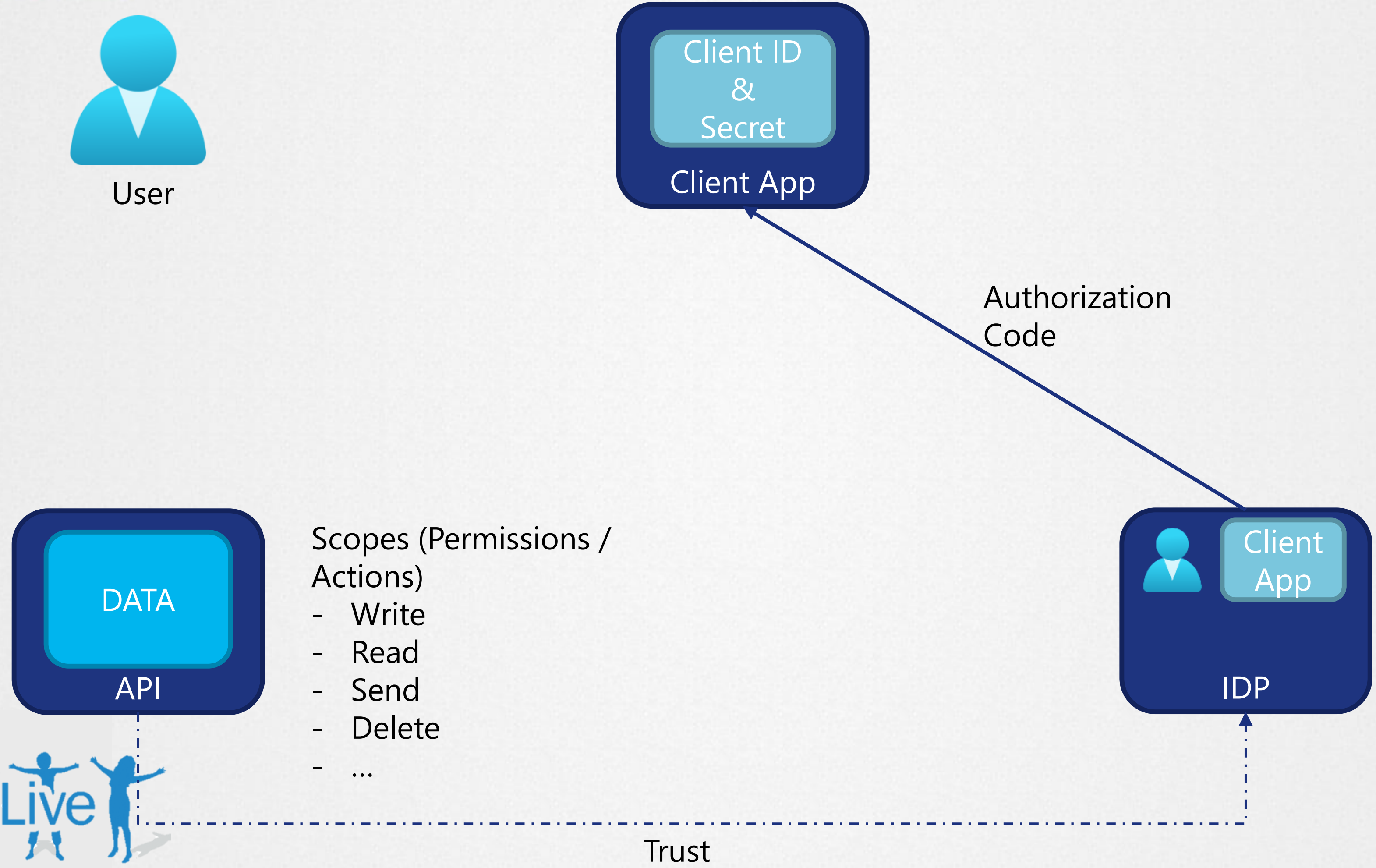
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Client
App

IDP

Trust



User

Client ID
&
Secret

Client App

Authorization
Code

DATA

API

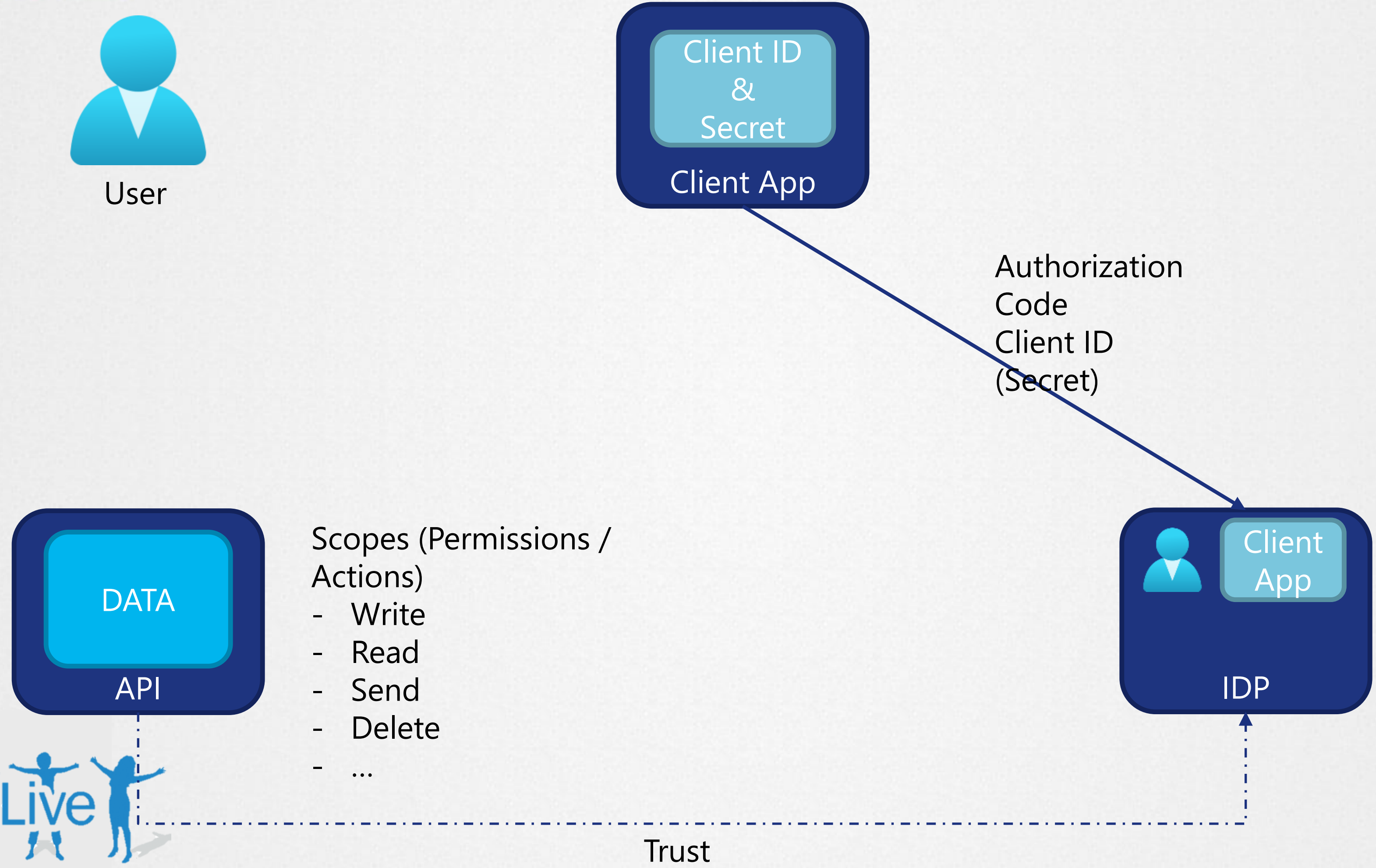
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Client
App

IDP

Trust



User

Client ID & Secret

Client App

Authorization Code
Client ID
(Secret)

Client App

IDP

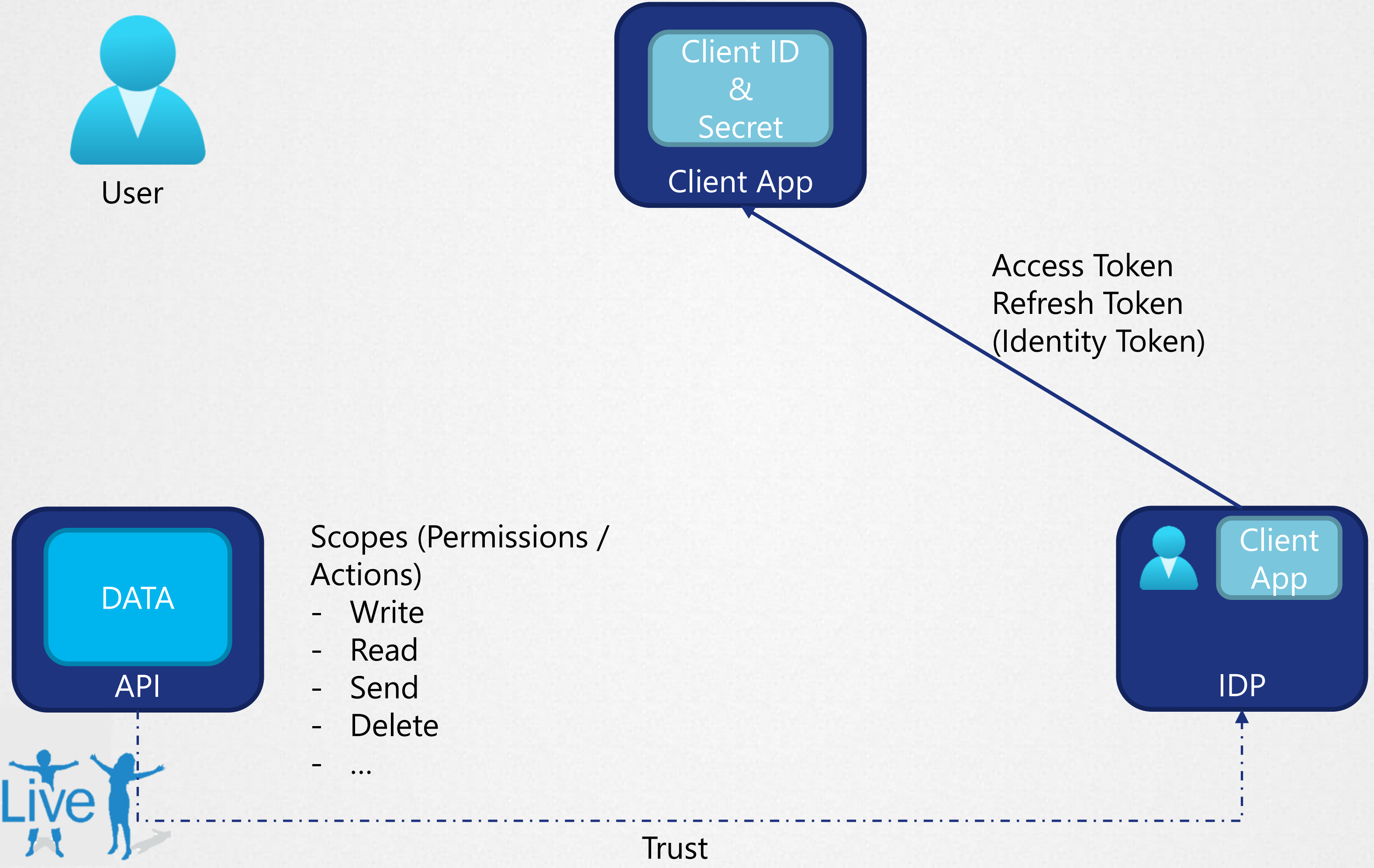
DATA

API

Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Trust



User

Client ID
&
Secret

Client App

Access Token
Refresh Token
(Identity Token)

DATA

API

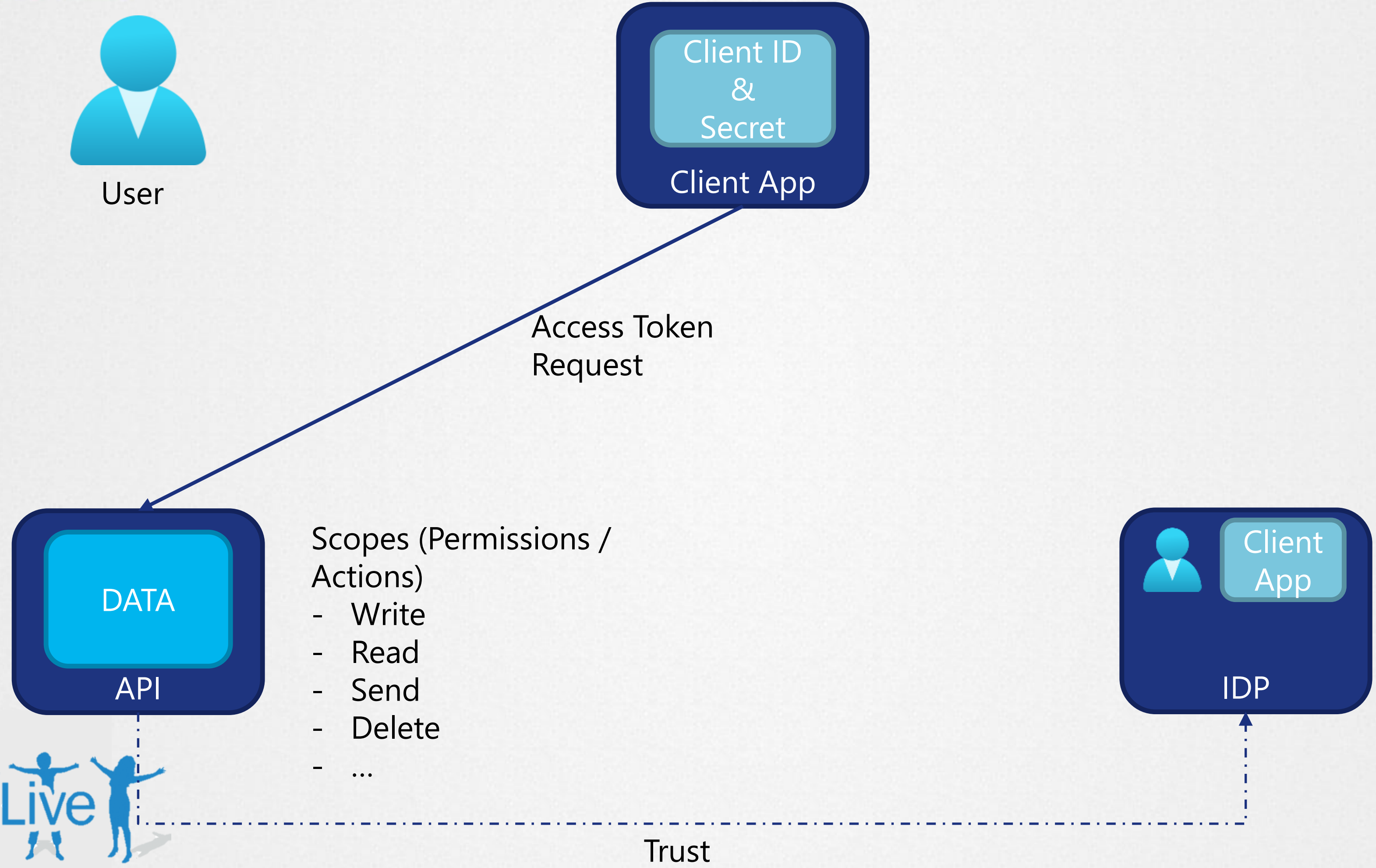
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Client App

IDP

Trust



User

Client ID
&
Secret

Client App

Access Token
Request

DATA

API

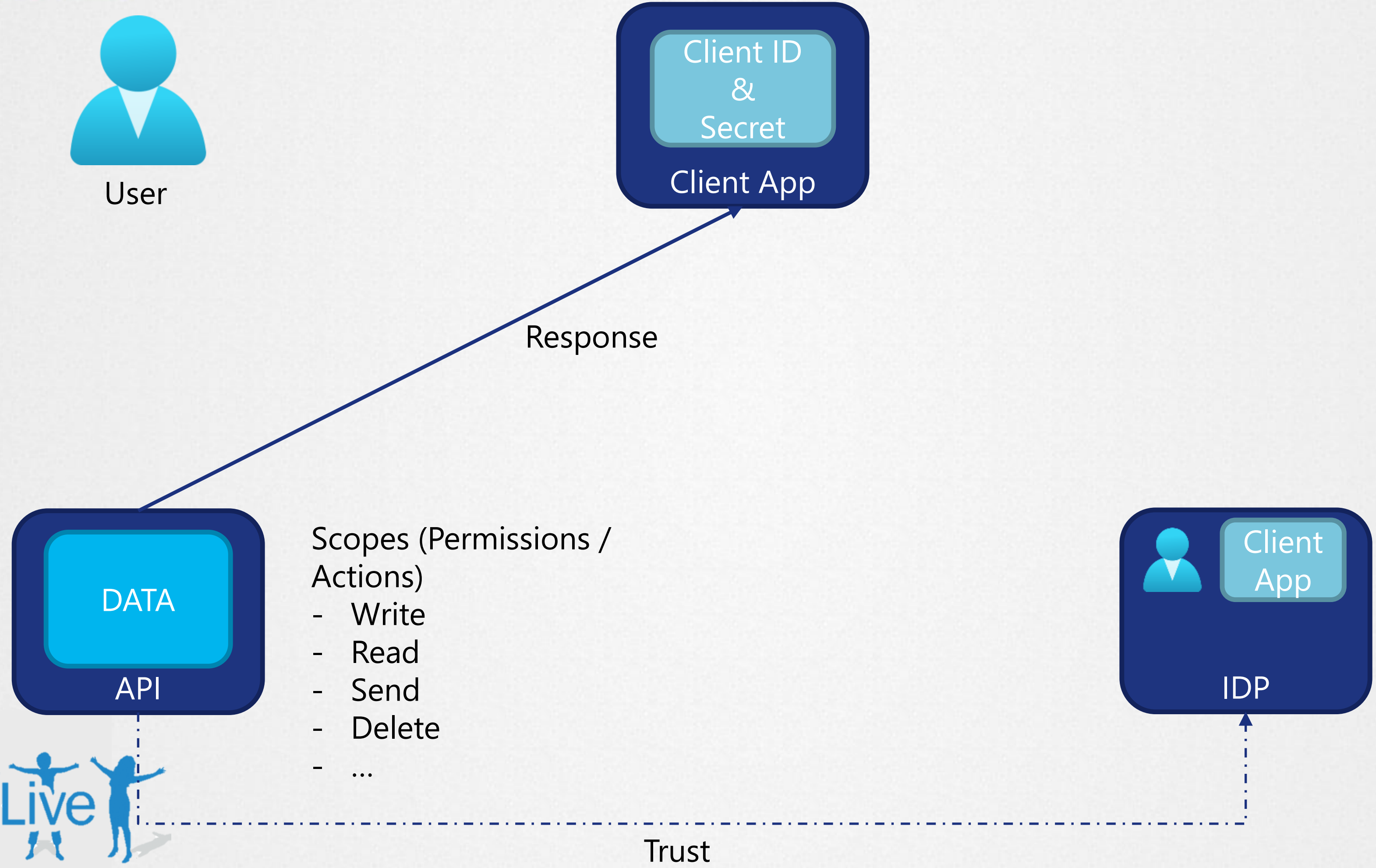
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Client
App

IDP

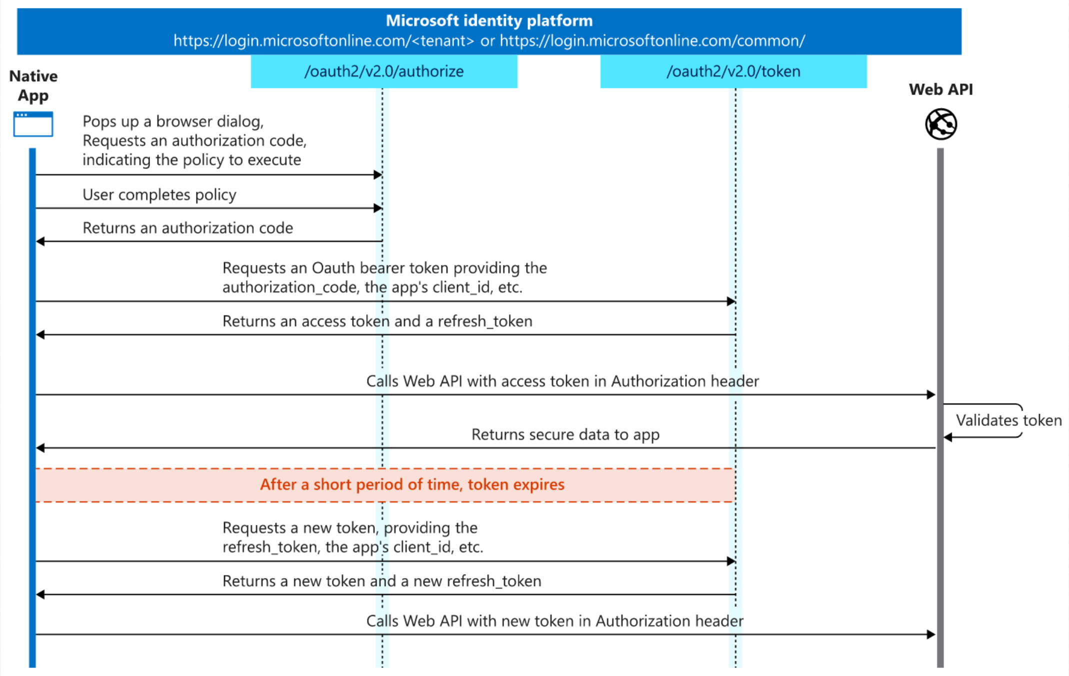
Trust



Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

This is how it flows … in AAD



Microsoft identity platform
https://login.microsoftonline.com/<tenant> or https://login.microsoftonline.com/common/

Pops up a browser dialog, Requests an authorization code, indicating the policy to execute

User completes policy

Returns an authorization code

Requests an Oauth bearer token providing the authorization_code, the app's client_id, etc.

Returns an access token and a refresh_token

Calls Web API with access token in Authorization header

Validates token

Returns secure data to app

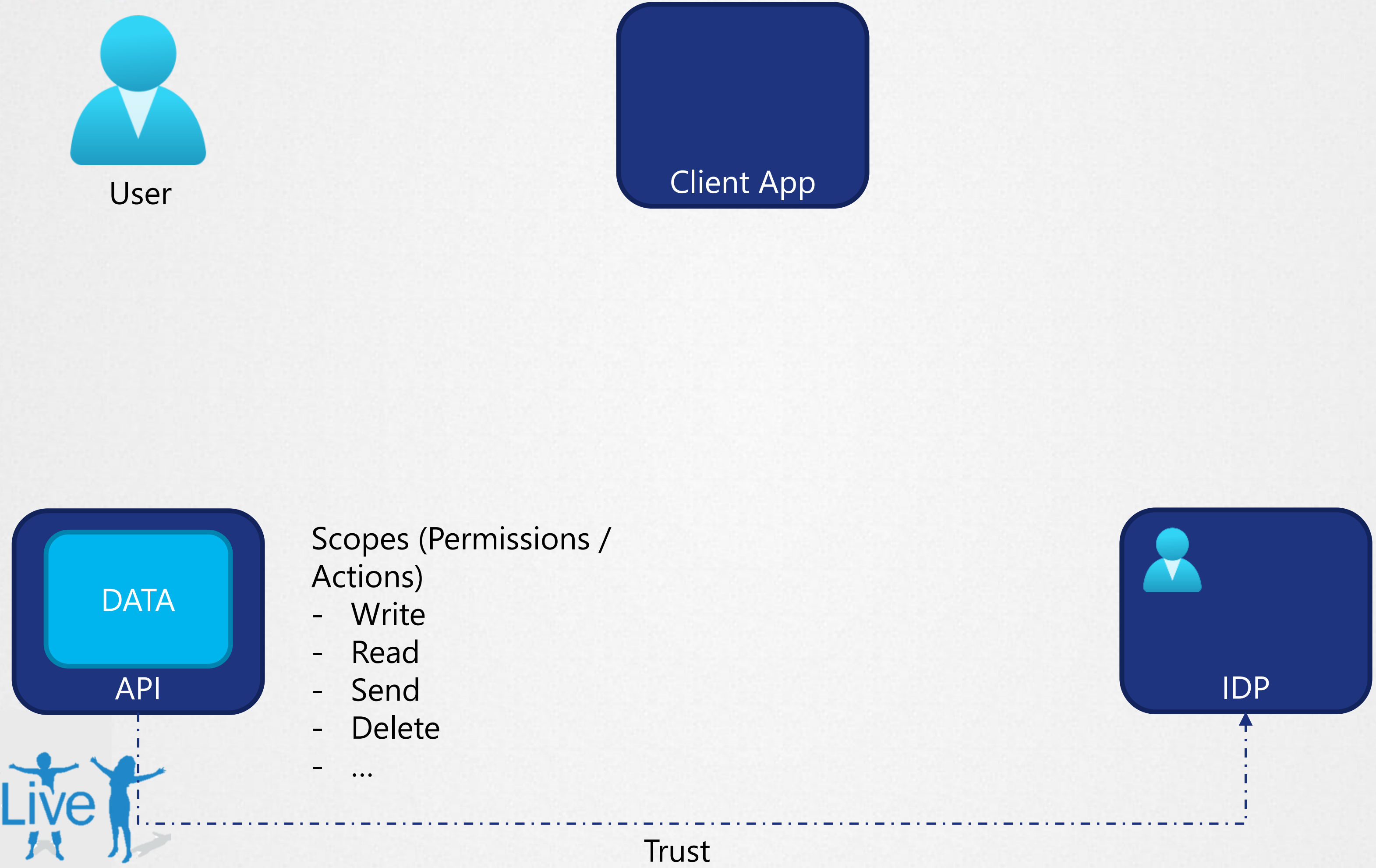
After a short period of time, token expires

Requests a new token, providing the refresh_token, the app's client_id, etc.

Returns a new token and a new refresh_token

Calls Web API with new token in Authorization header

And what about AAD now?



User

Client App

DATA

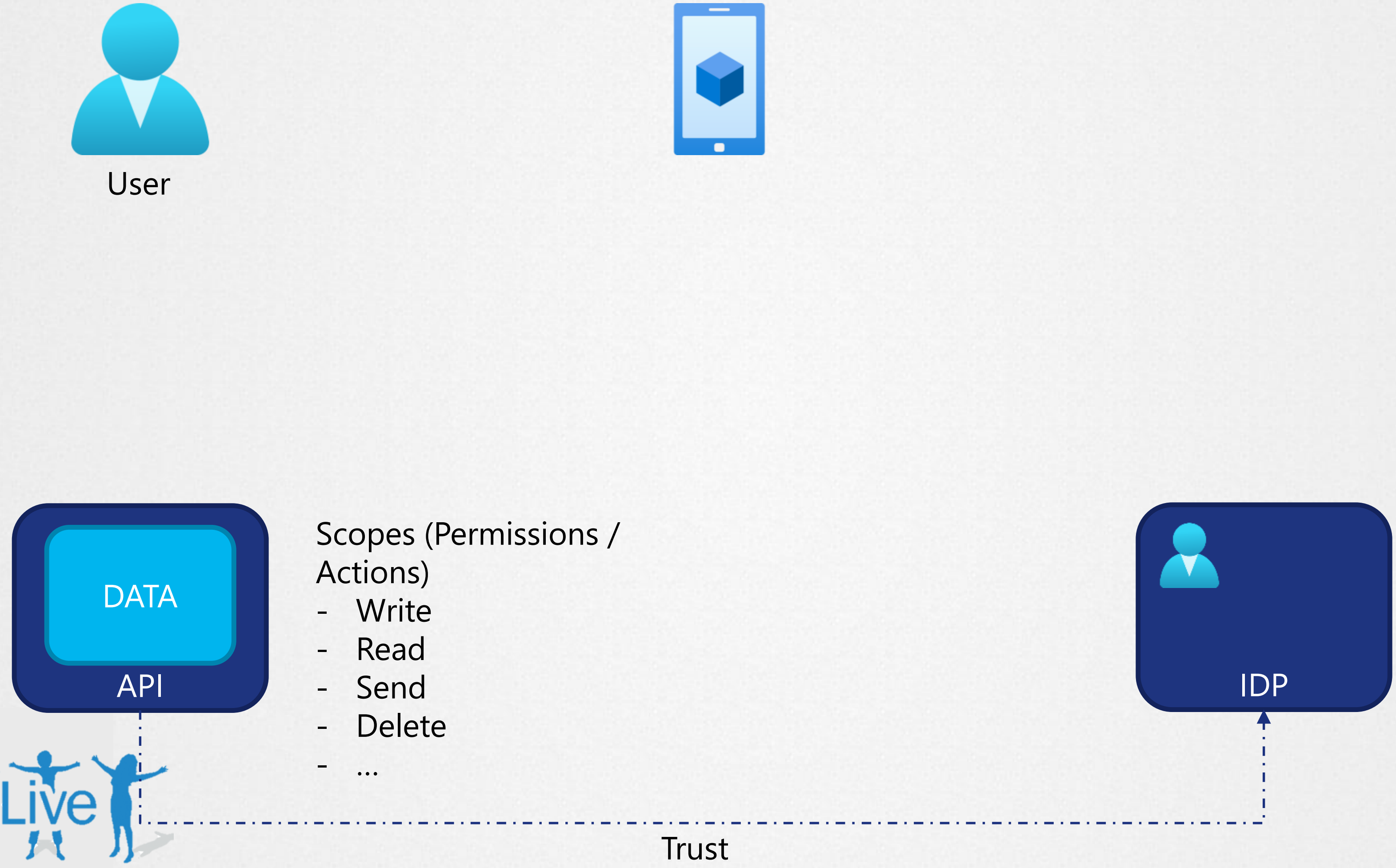
API

Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

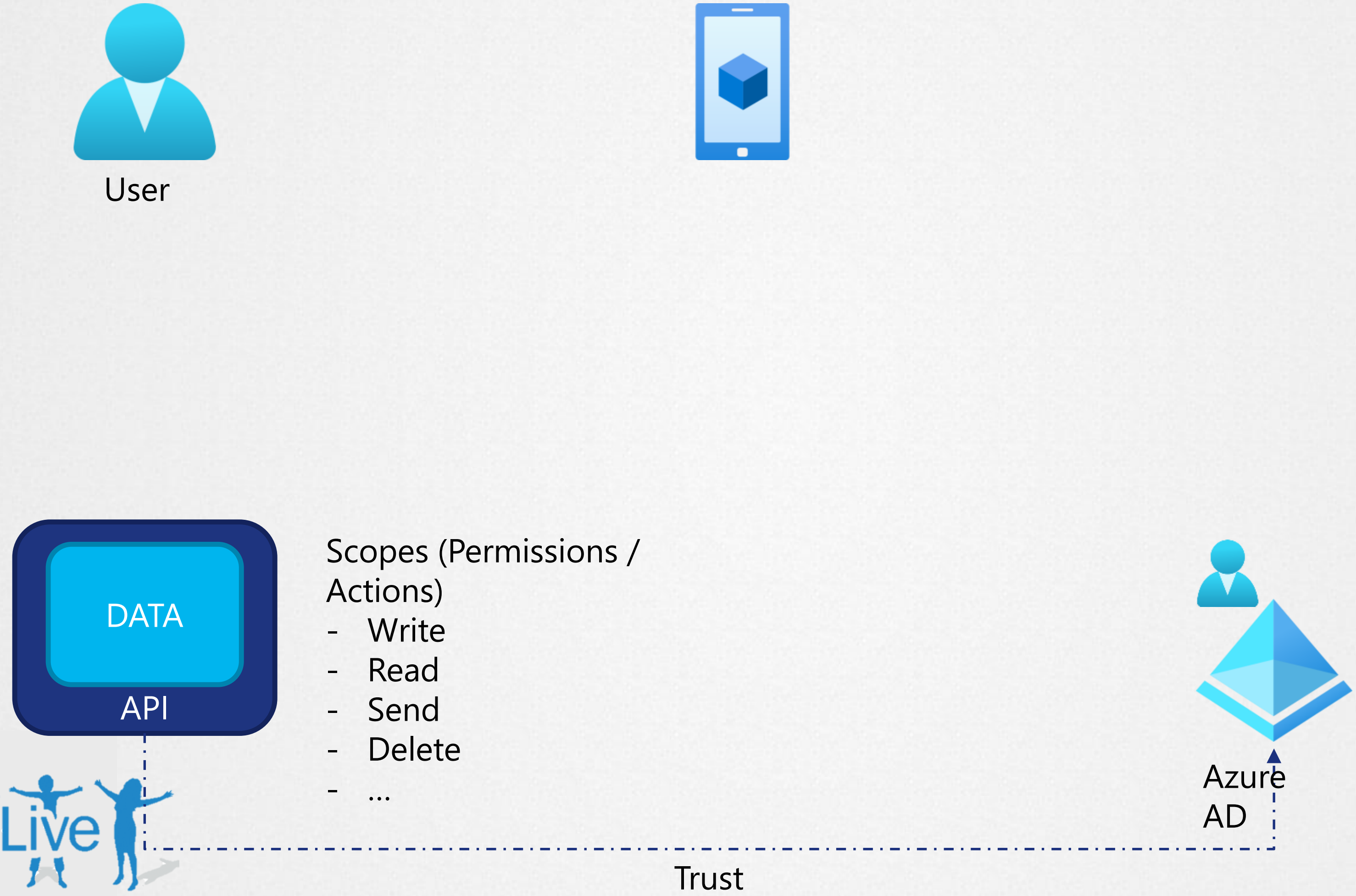
IDP

Trust



Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...



User

DATA

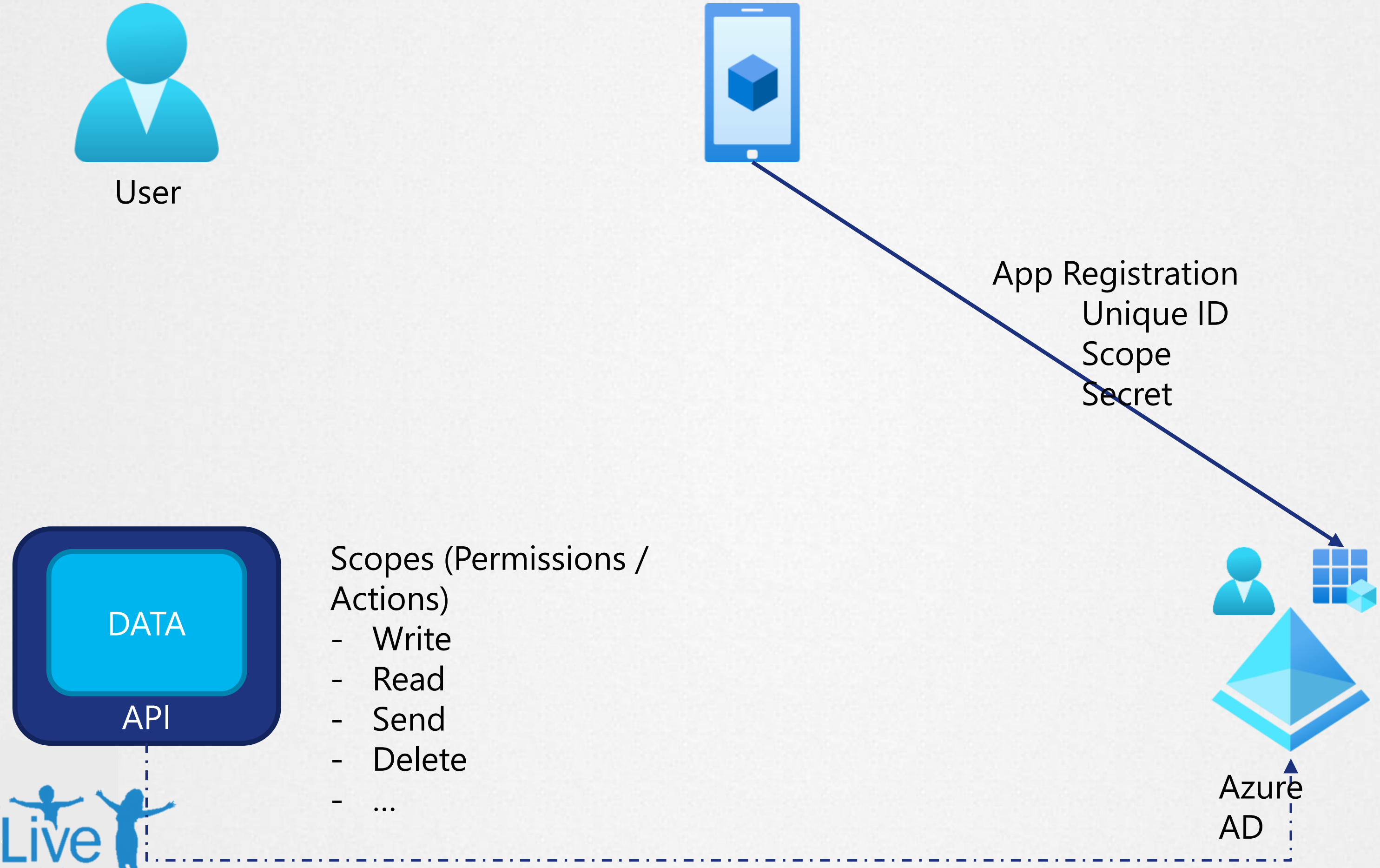
API

Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- ...

Azure AD

Trust



User

App Registration

Unique ID

Scope

Secret

DATA

API

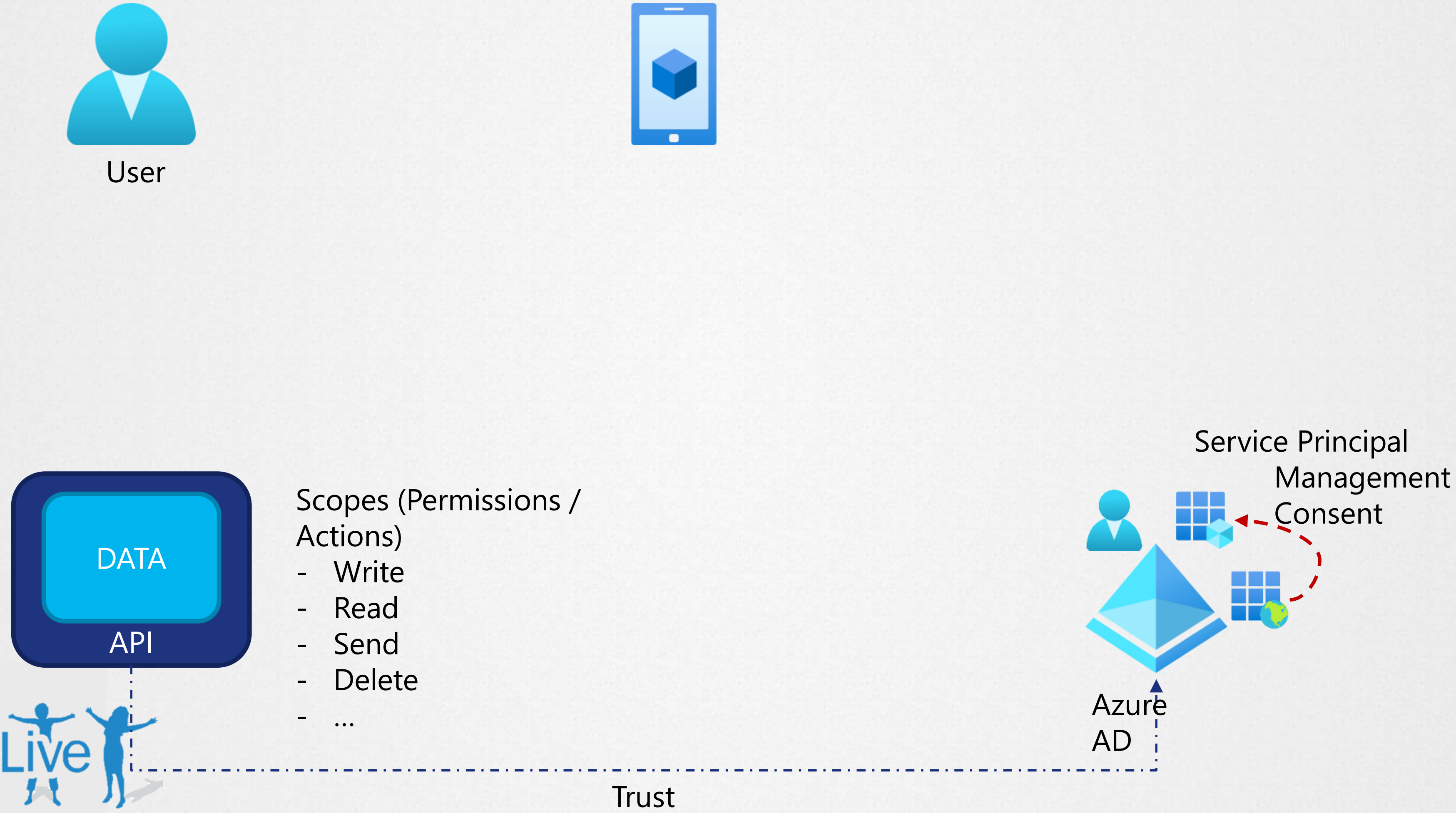
Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Azure AD

Trust

DEMO?!



User

DATA

API

Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

Service Principal

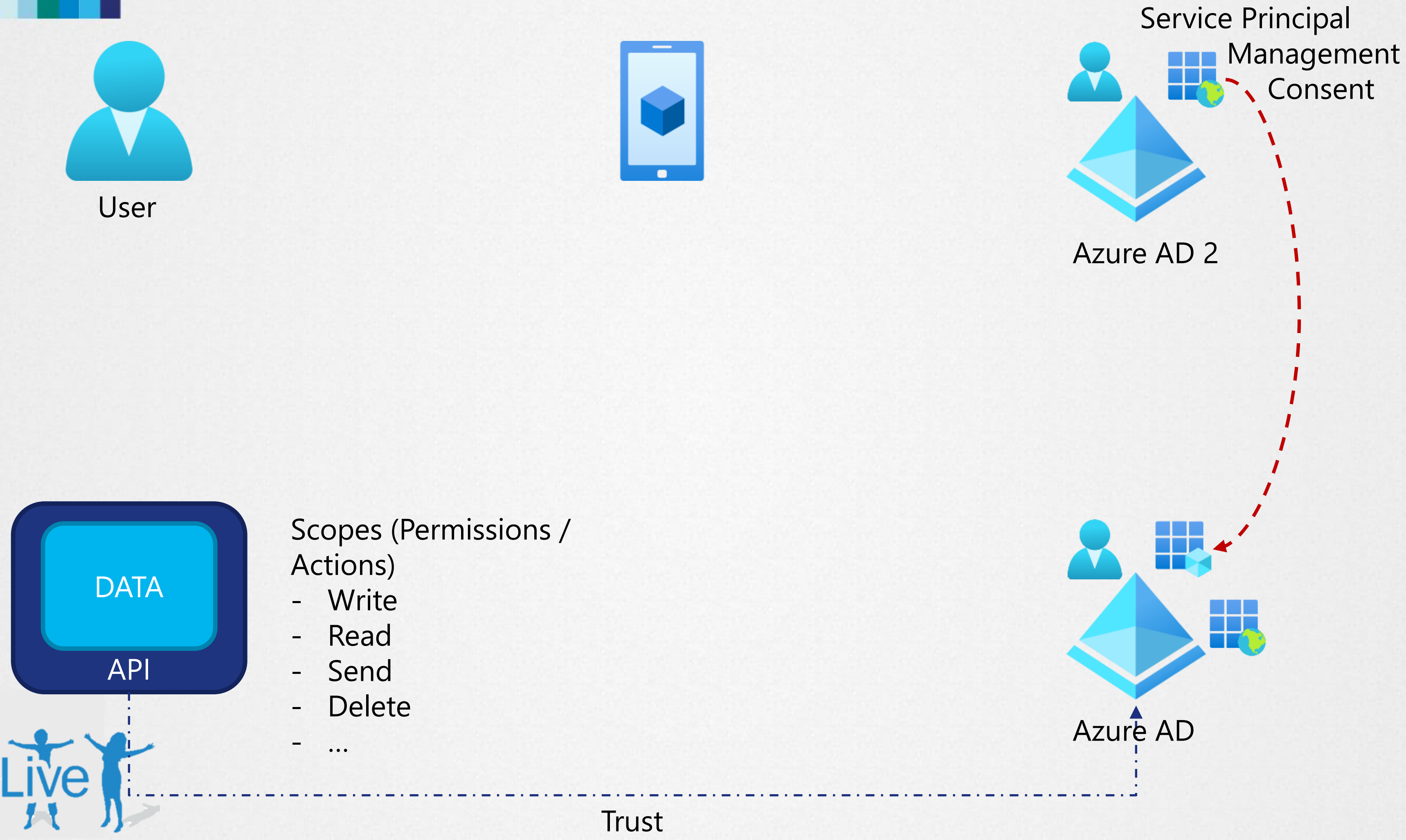
Management

Consent

Azure AD

Trust

DEMO?!



Service Principal
Management
Consent

User

Azure AD 2

DATA

API

Azure AD

Trust

Scopes (Permissions / Actions)

- Write
- Read
- Send
- Delete
- …

How to define it?

Application Object – App Registration

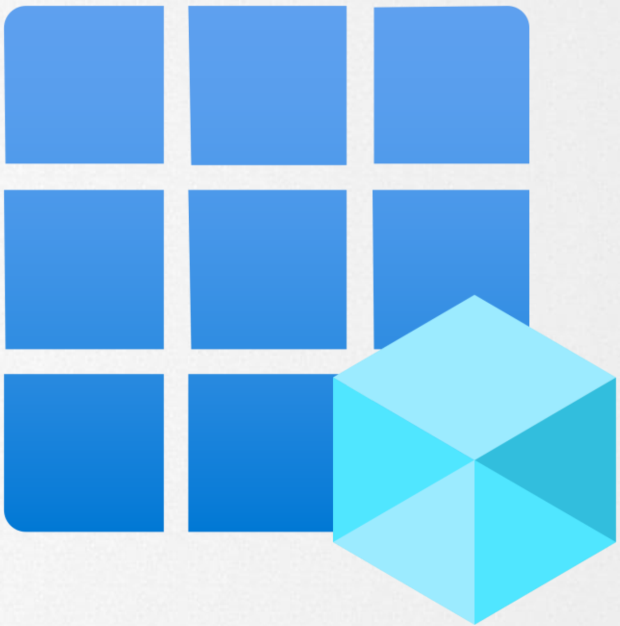
Created in “Home tenant”

App Registration stays here

App Object used as blueprint to create service principals in every tenant the app is used

Defines 3 aspects

- How to issue tokens
- Resource access
- Actions



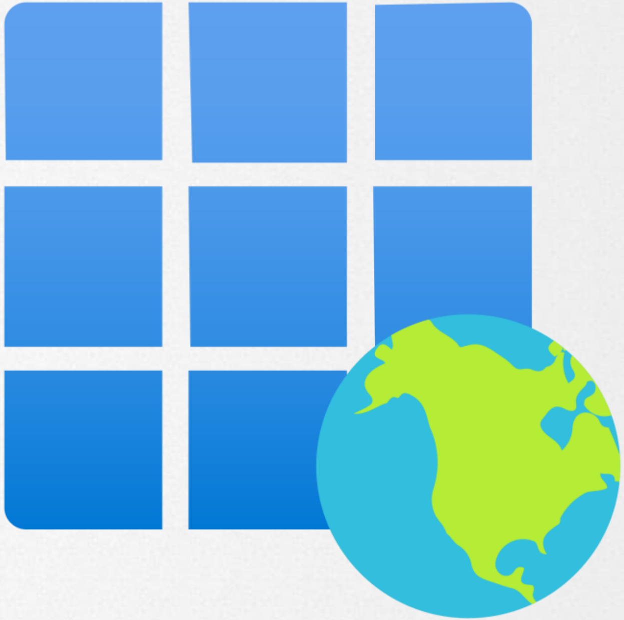
Service Principal Object – Enterprise App

To access resources secured by AAD you need entity represented by security principal

- Users = user principal
- Applications = service principal

Security principal defines

- Access policy
- Permissions



Service Principal Object – Types

- Application
  - Representation of an app object from a single tenant
  - SPO defines what app can do, who can access, and resource access
- Managed Identity
  - Auto-managed inside Azure
  - Linked to Azure Resource
  - System or User Assigned
- Legacy
  - Legacy was created before app registration
  - Only used in tenant where it was created

How to use it?

Create them

- App registration
  - Create AAD Integration
  - Portal
  - PowerShell / CLI / Graph
- Enterprise App
  - IT Admin
  - Log in to 3rd party app
  - Consent

DEMO?!

Use them

Access 3rd Party Apps

- e.g. Calendly, Sessionize or others

Assign roles in Azure

- e.g. KeyVault Access, Resource Graph or

Allow graph access

- e.g. Profile, Mail or Calendar

Service Connections

- e.g. Azure DevOps, Management Tools or DevTools

Best Practices?!

Best Practices

- Redirect URIs
  - Ownership of URIs
  - HTTPS
  - Avoid wildcatds
  - Manage and Monitor DNS
- Authentication
  - Avoid implicit flows
  - If not used → remove

Best Practices

- Certificates & Secrets
  - Prefer Certs over Secrets
  - Use KeyVault with Managed Identity
  - Rollover and check usage
  - Check repos
  - Use Credential Scanner
- Owners
  - Review and Manage owners

Thank you!
See you in Erfurt?

Experts Live Germany

Thanks to our Sponsors!

ACP IT for innovators.

Microsoft

NiCE
IT Management Solutions
www.nice.de

THOMAS
KRENN®

veeam

secureguard

ACP IT for innovators.

Live