Eric Berg

Vice President Consulting Expert @ CGI

MVP Azure & CDM, LinkedIn Learning Trainer

Cloud, Datacenter & Management

info@ericberg.de

@ericberg_de | @GeekZeugs

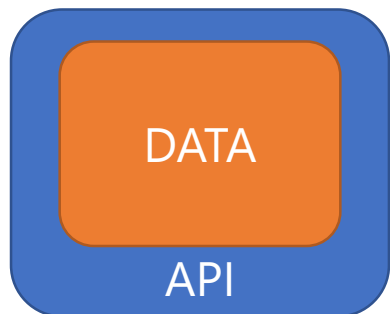www.ericberg.de | www.geekzeugs.de

What is it all about?

User

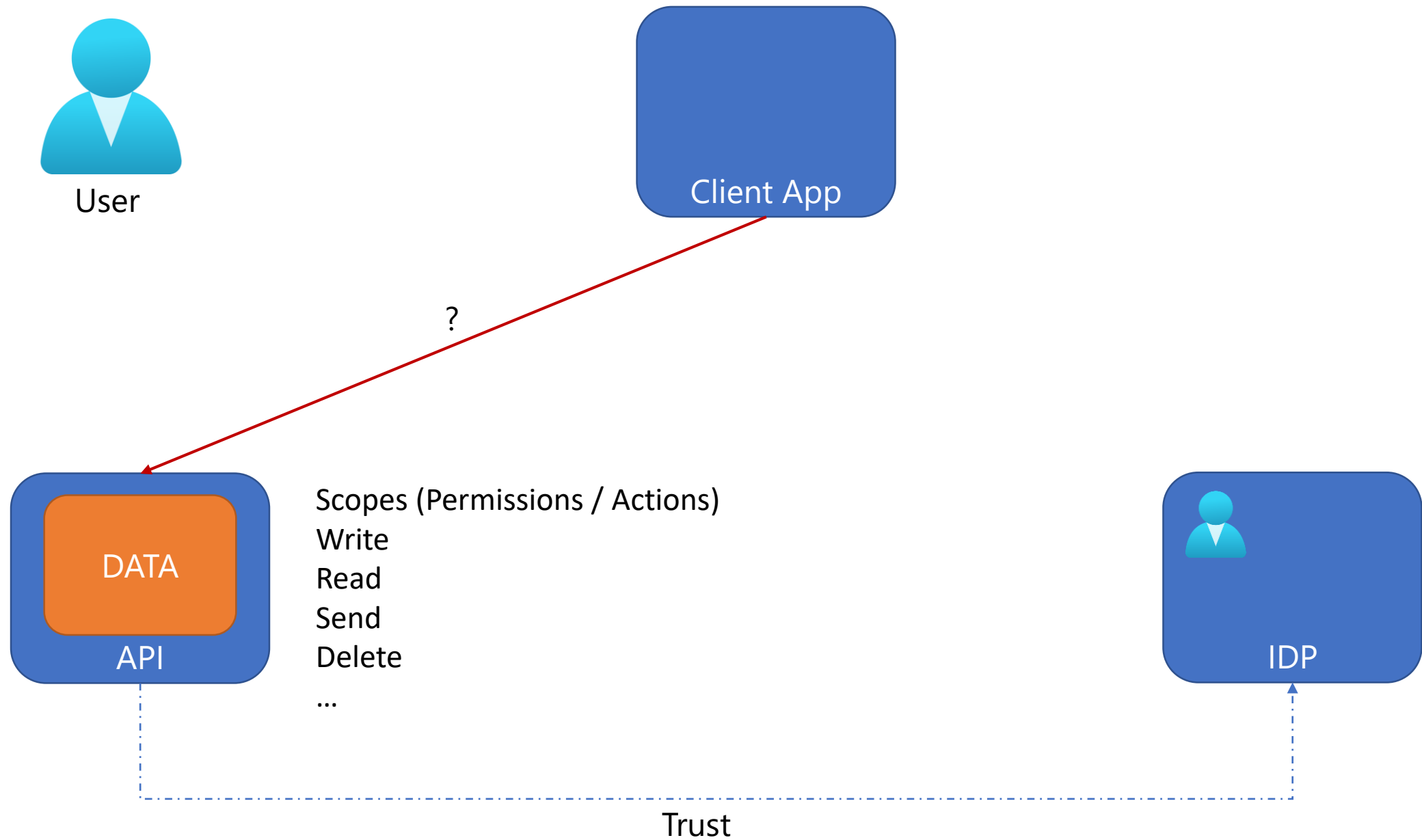Client App

DATA

API

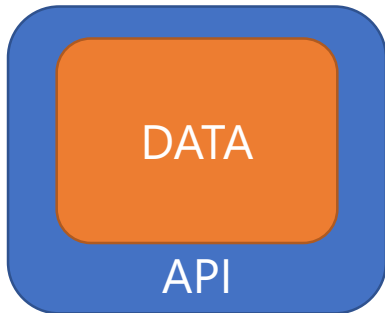Scopes (Permissions / Actions)
Write
Read
Send
Delete
…

IDP

Trust

User

Client App

?

Scopes (Permissions / Actions)
Write
Read
Send
Delete
...
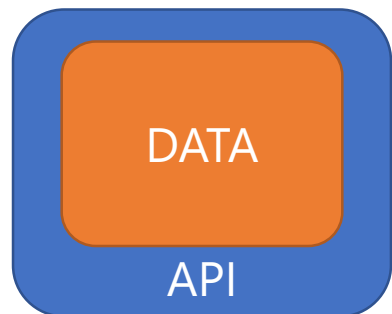
DATA

API

IDP
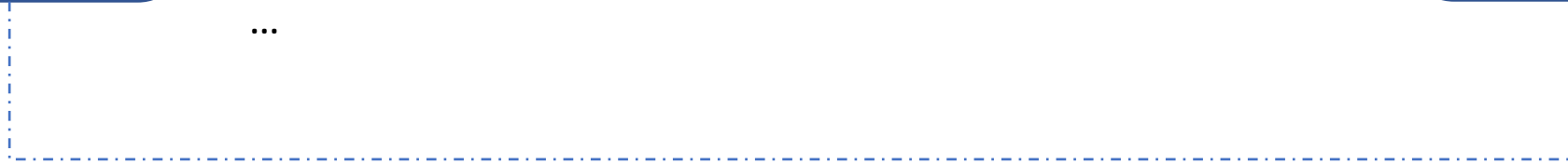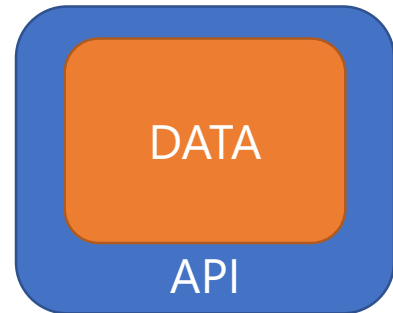
Trust

This is how it flows … in AAD

The following diagram shows the ROPC flow.

How to do it better?

User

Client ID
&
Secret

Client App

Response

Scopes (Permissions / Actions)
Write
Read
Send
Delete
…

DATA

API

Client App

IDP
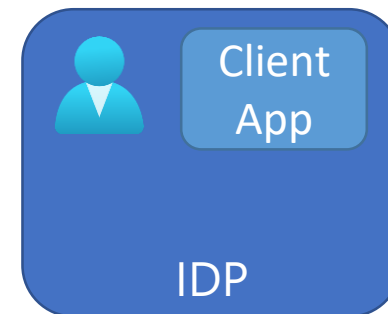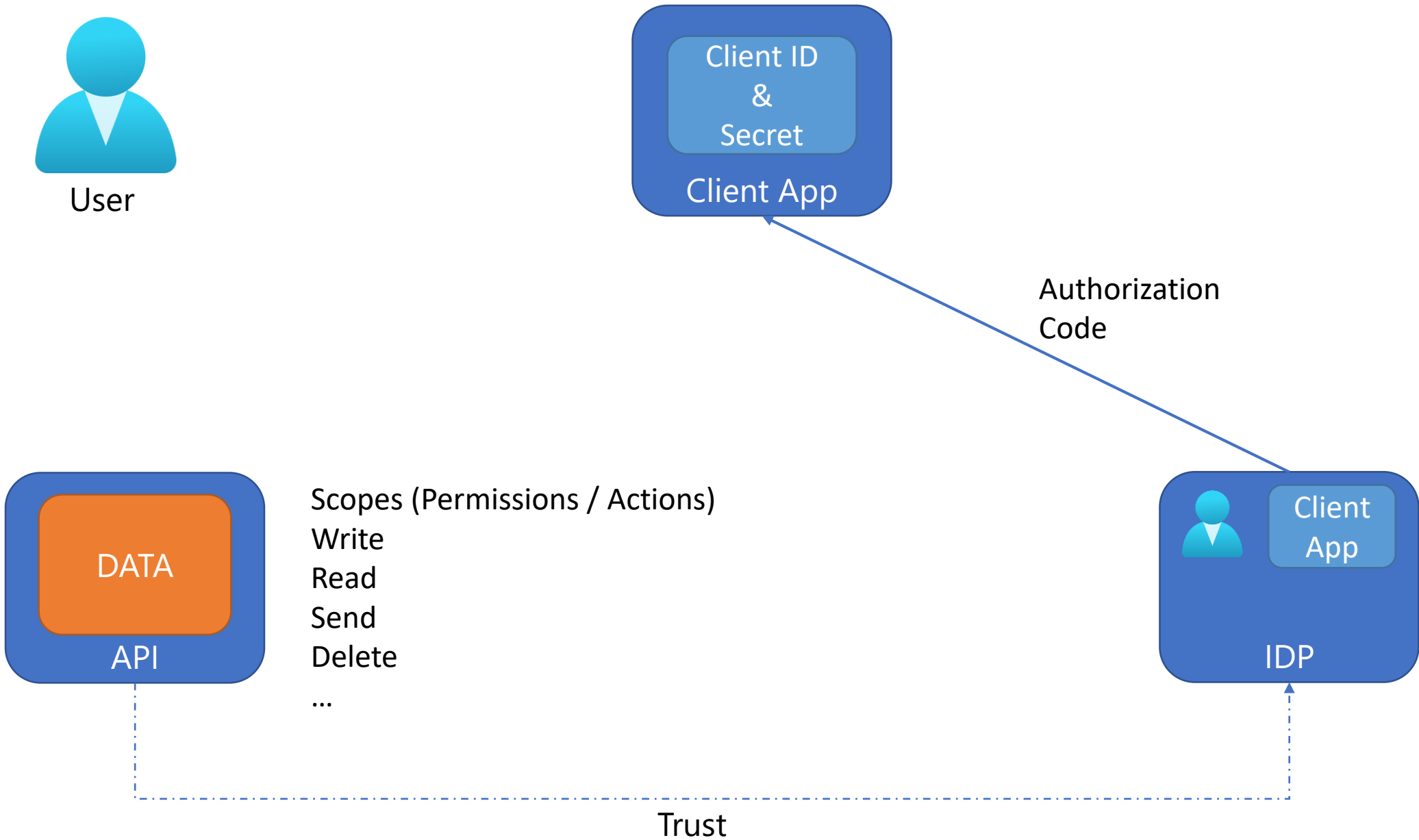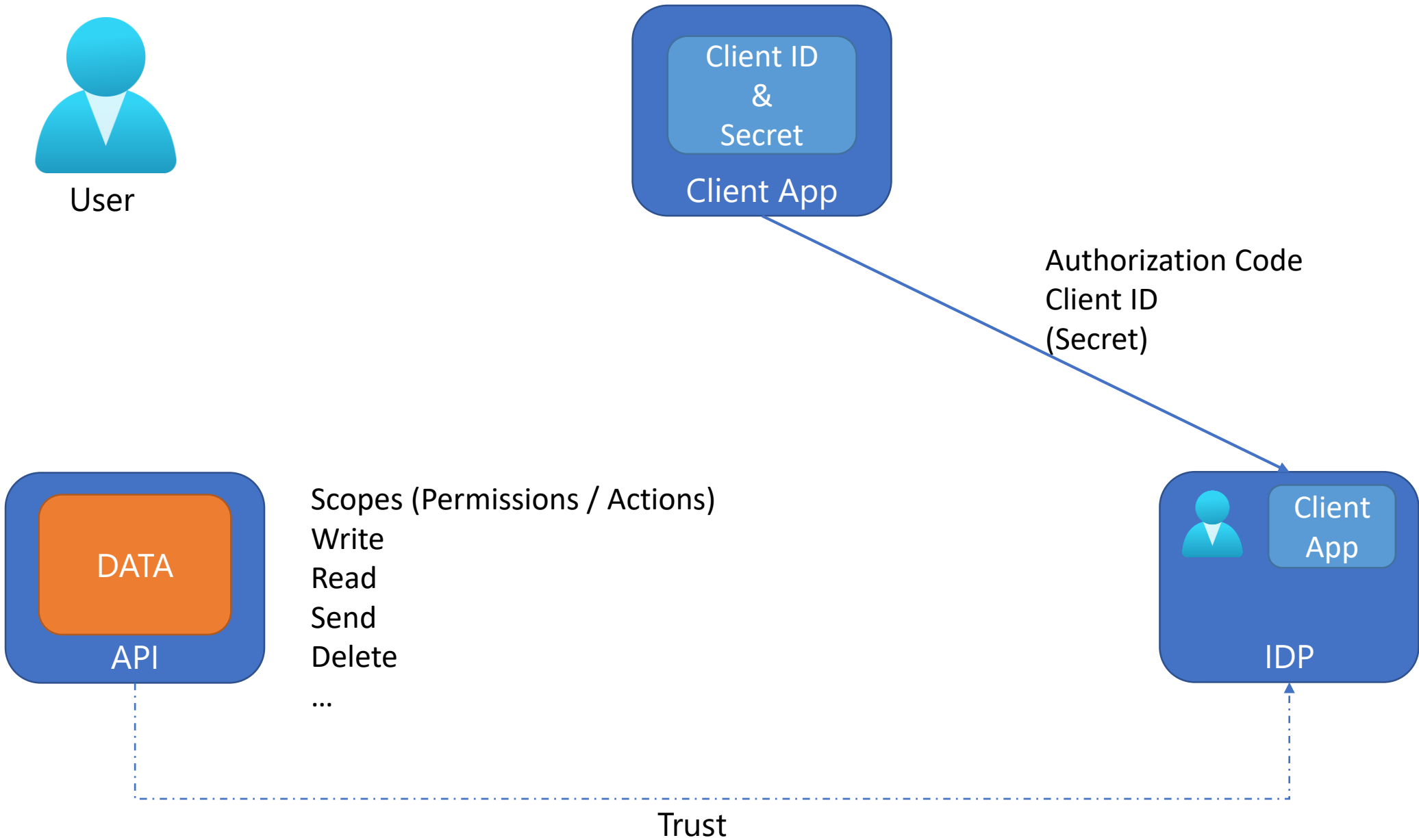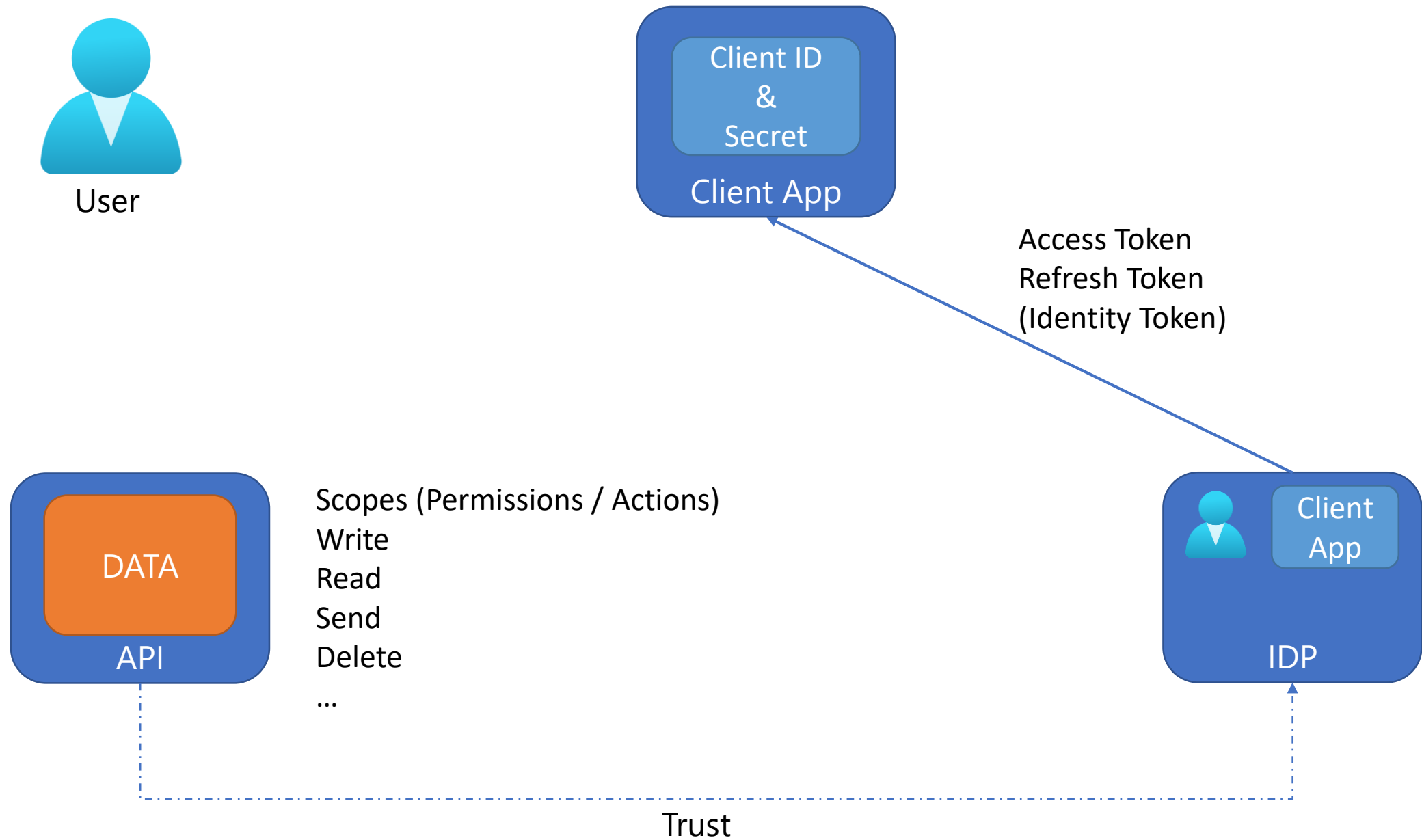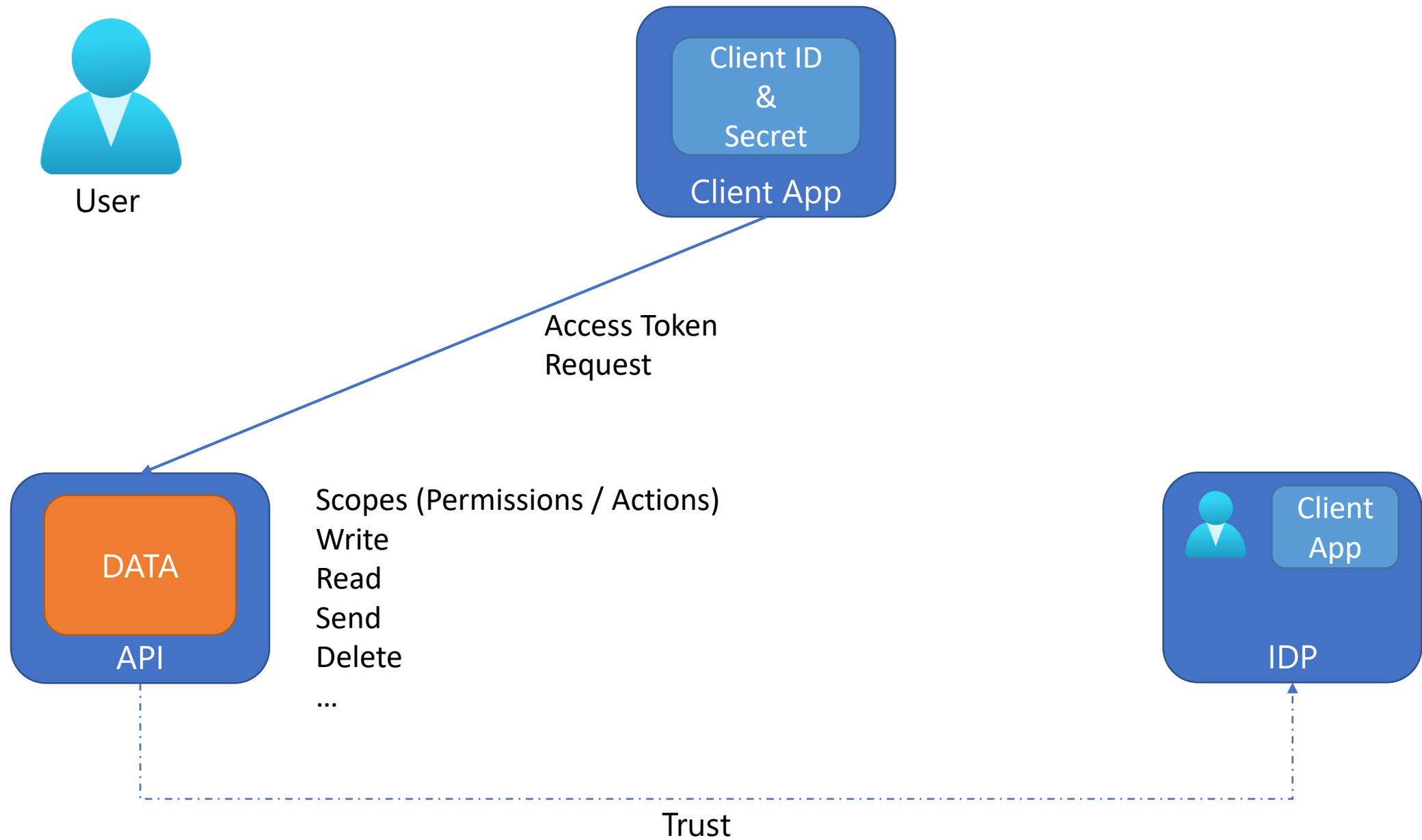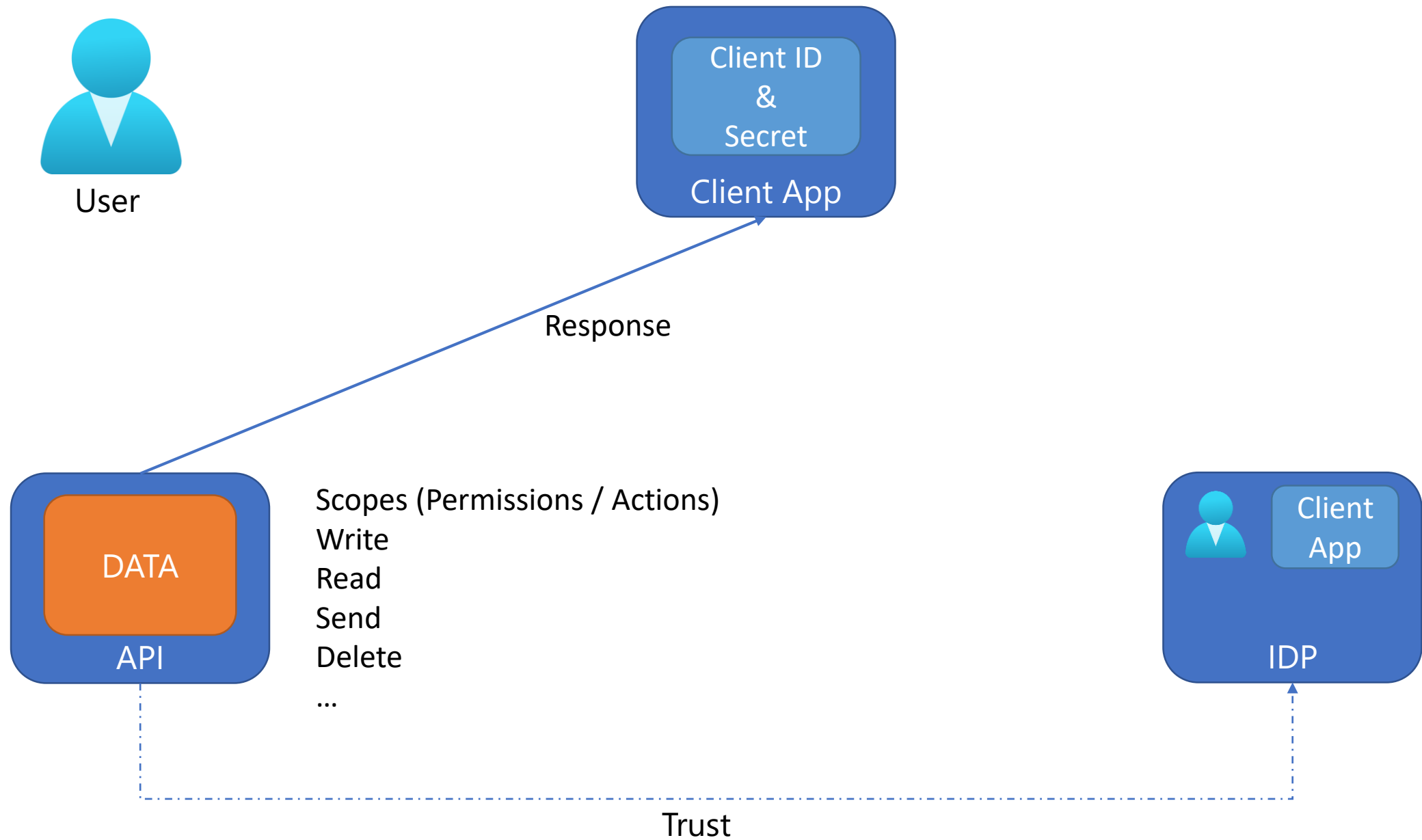
Trust

This is how it flows … in AAD
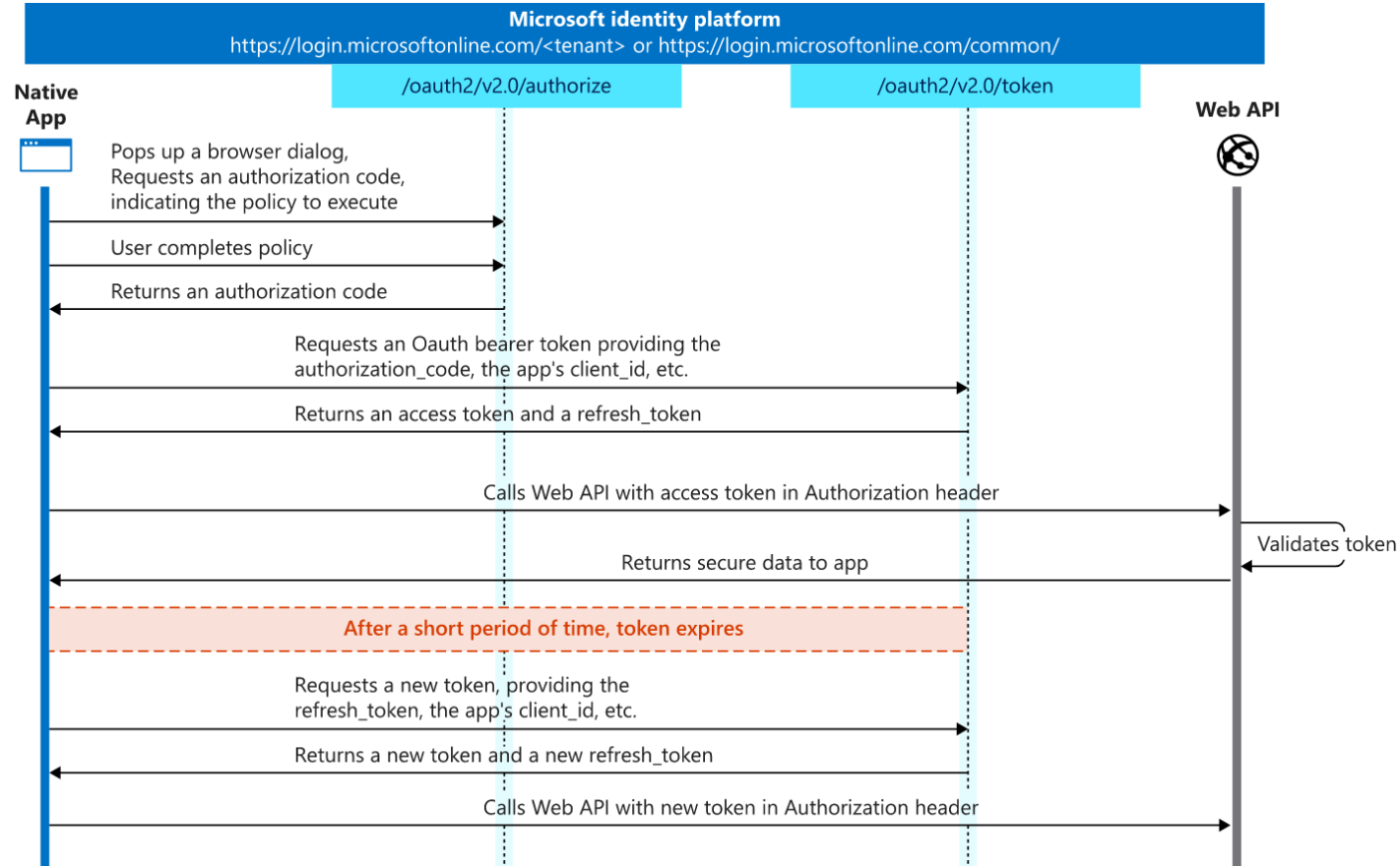
And what about AAD now?

User
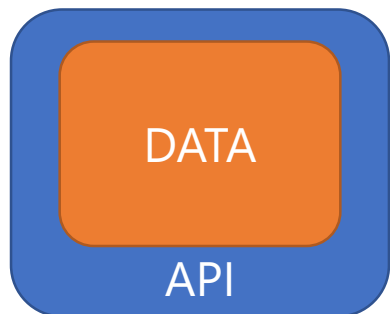
Scopes (Permissions / Actions)
Write
Read
Send
Delete
…
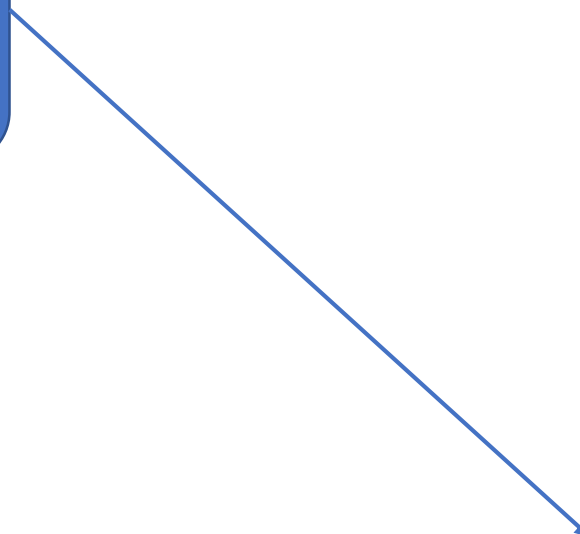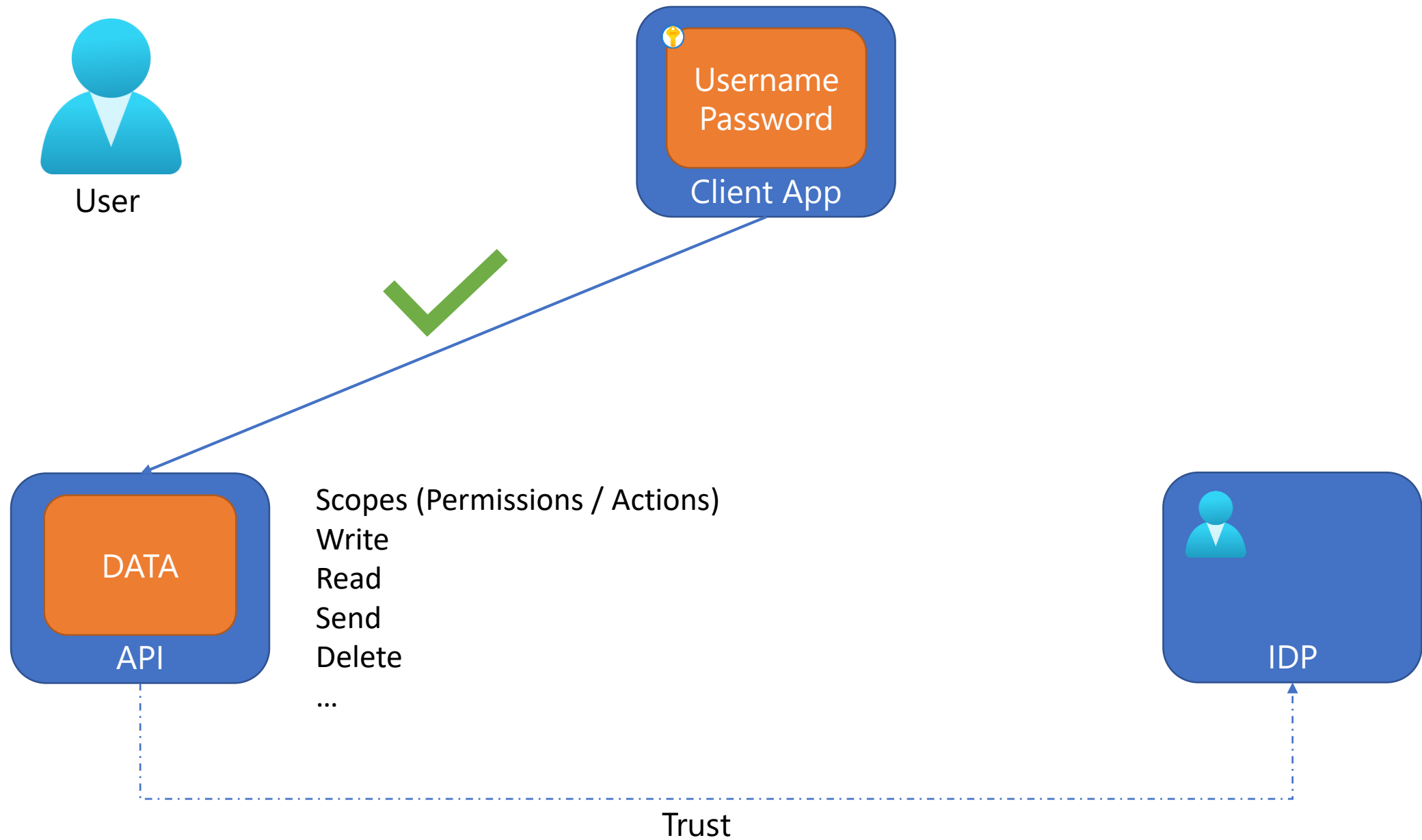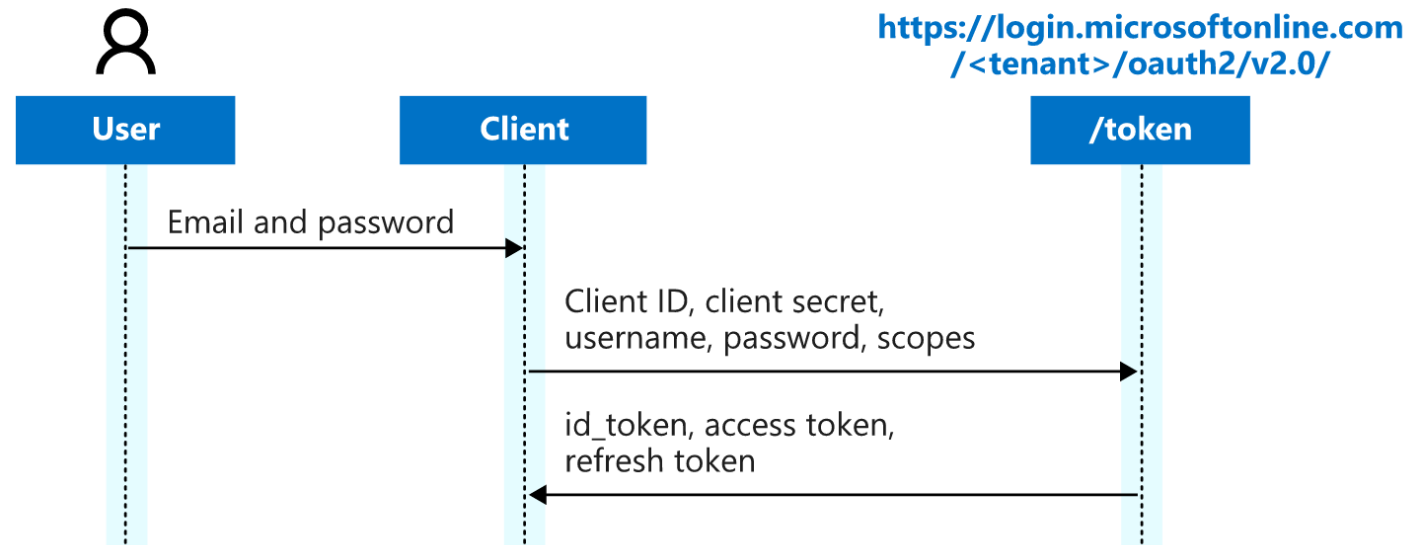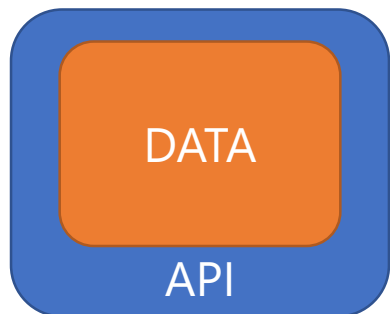
DATA
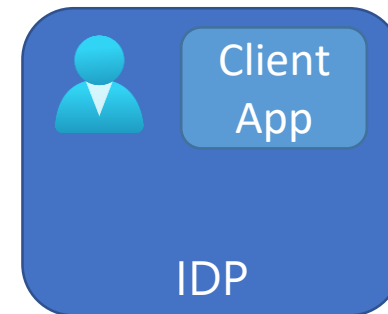
API

IDP

Trust

User

DATA
API
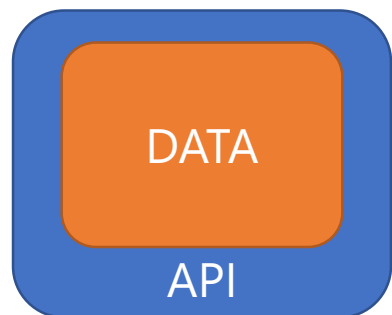
Scopes (Permissions / Actions)
Write
Read
Send
Delete
…

Azure AD

Trust

DEMO?!
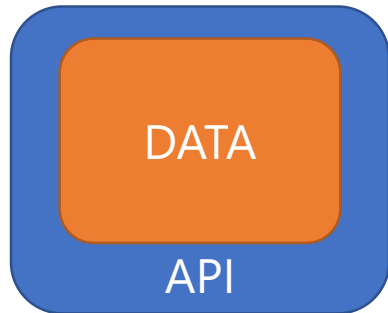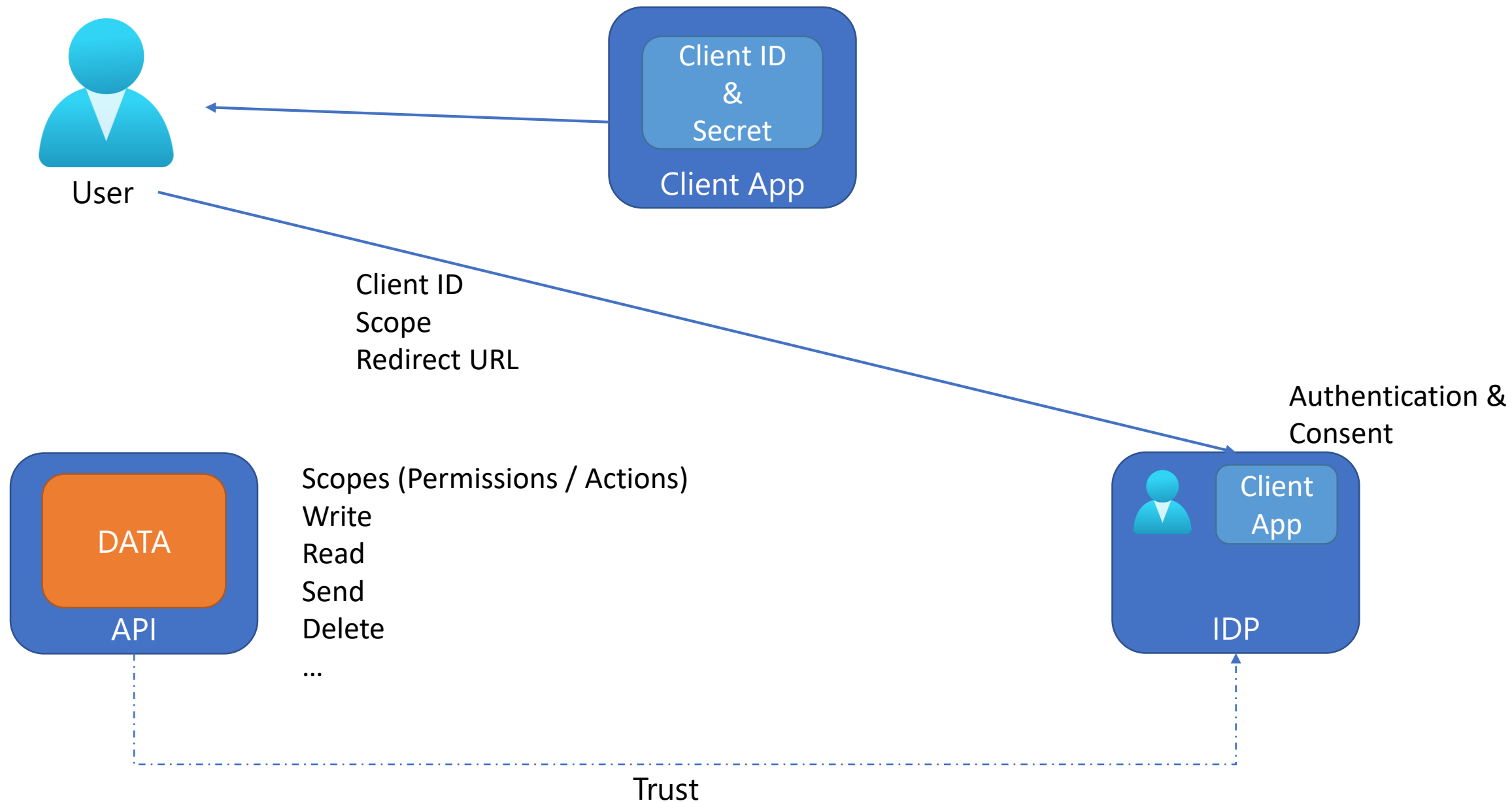
User

Scopes (Permissions / Actions)
Write
Read
Send
Delete
…
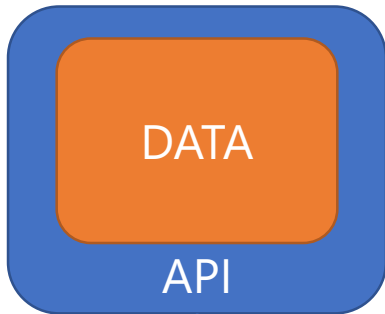
DATA

API

Service Principal
Management
Consent

Azure AD

Trust

DEMO?!

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
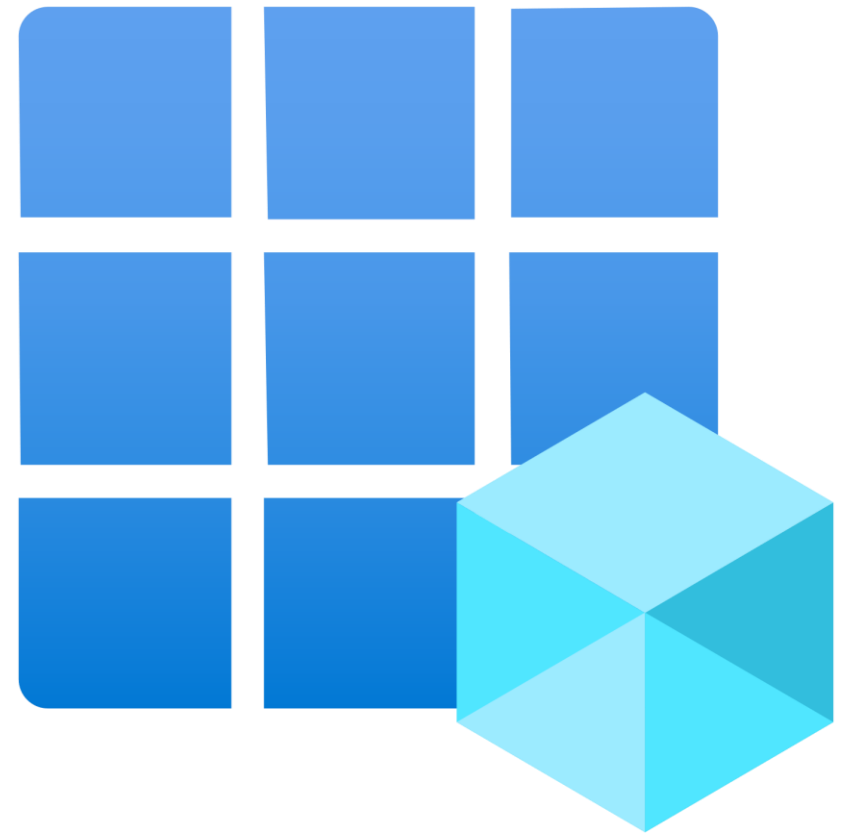
Service Principal Object – Enterprise App

- 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 wildcards
    - 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!

Questions?