Service Principals, App Registrations and other Azure Myths

- Eric Berg
- VP Expert @ CGI
- @ericberg_de
- MVP Azure & CDM

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —

Eric Berg

NORDIC
– VIRTUAL SUMMIT –

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

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

...

NORDIC
– VIRTUAL SUMMIT –
PATCH MY PC
RECAST SOFTWARE

What is it all about?

User

Client App

DATA

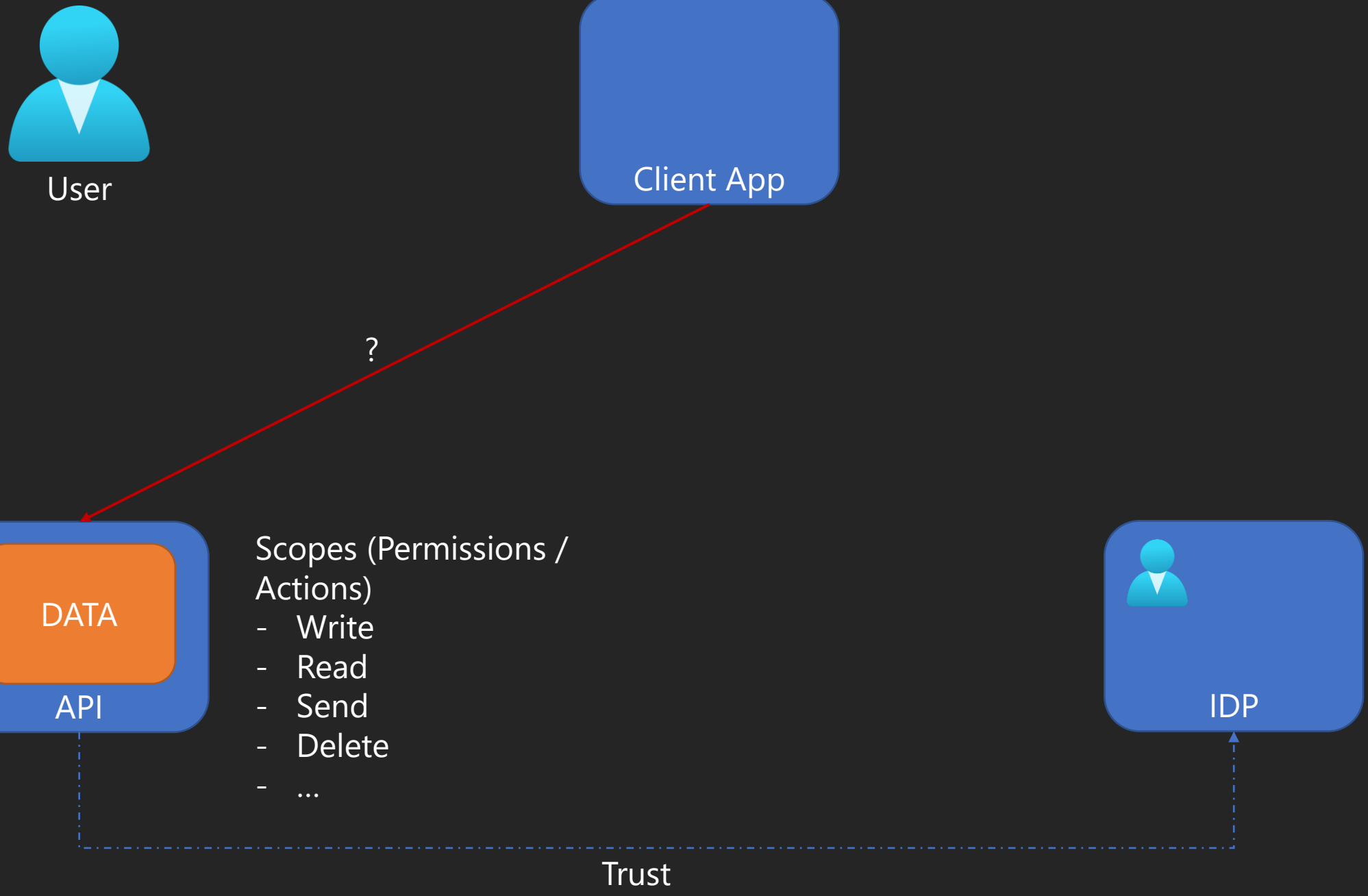
API

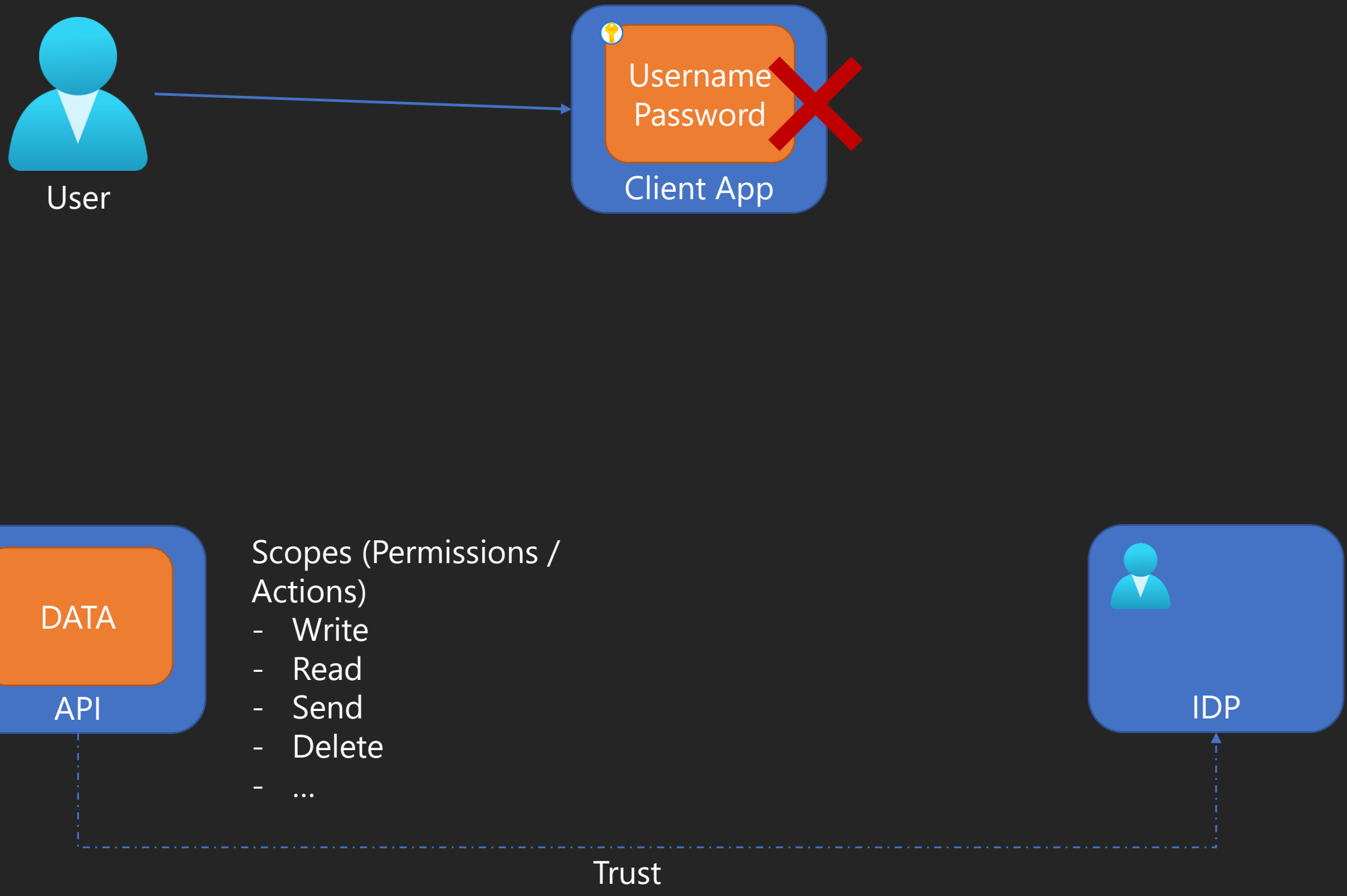
Scopes (Permissions / Actions)

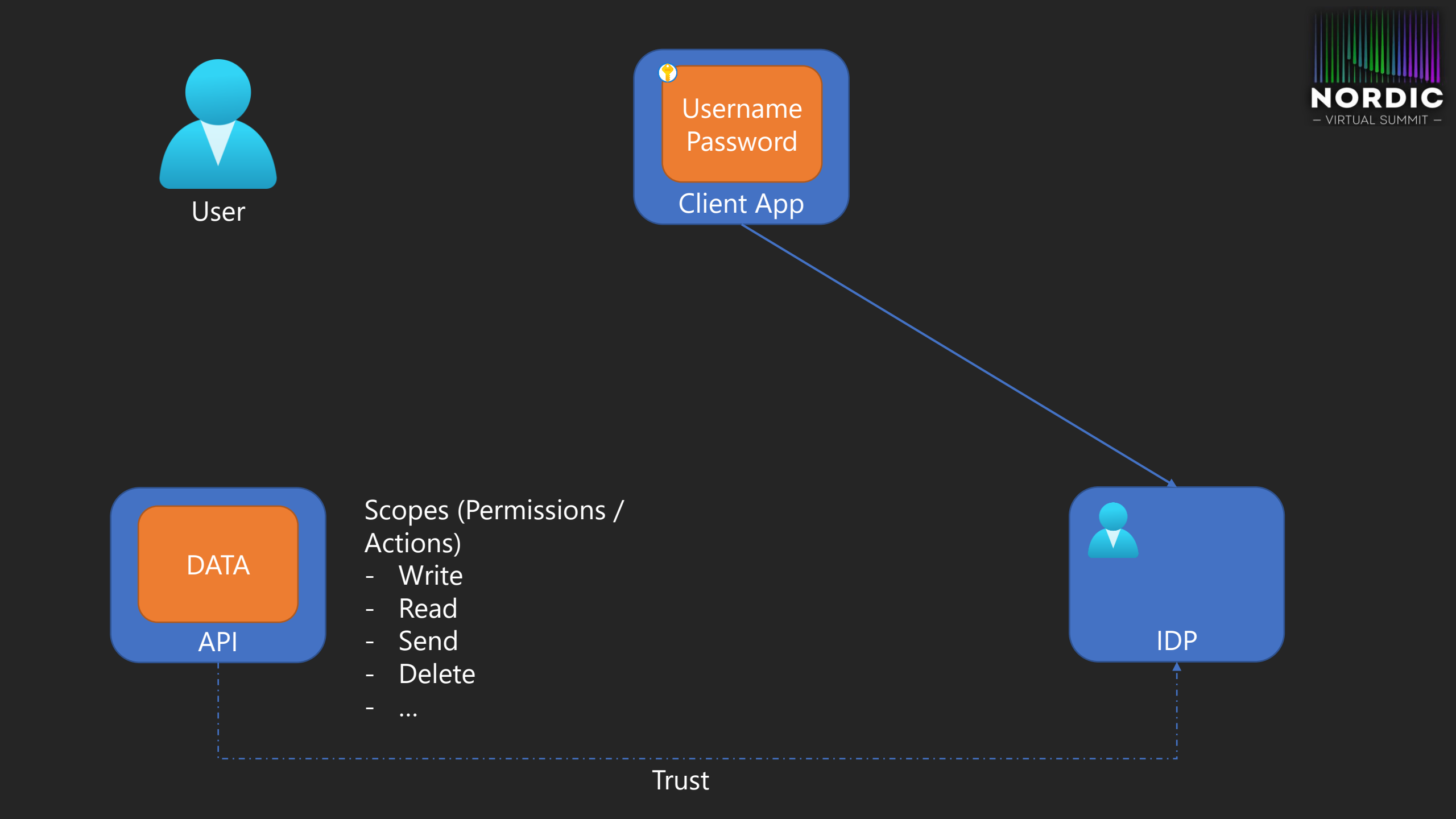
- Write
- Read
- Send
- Delete
- ...

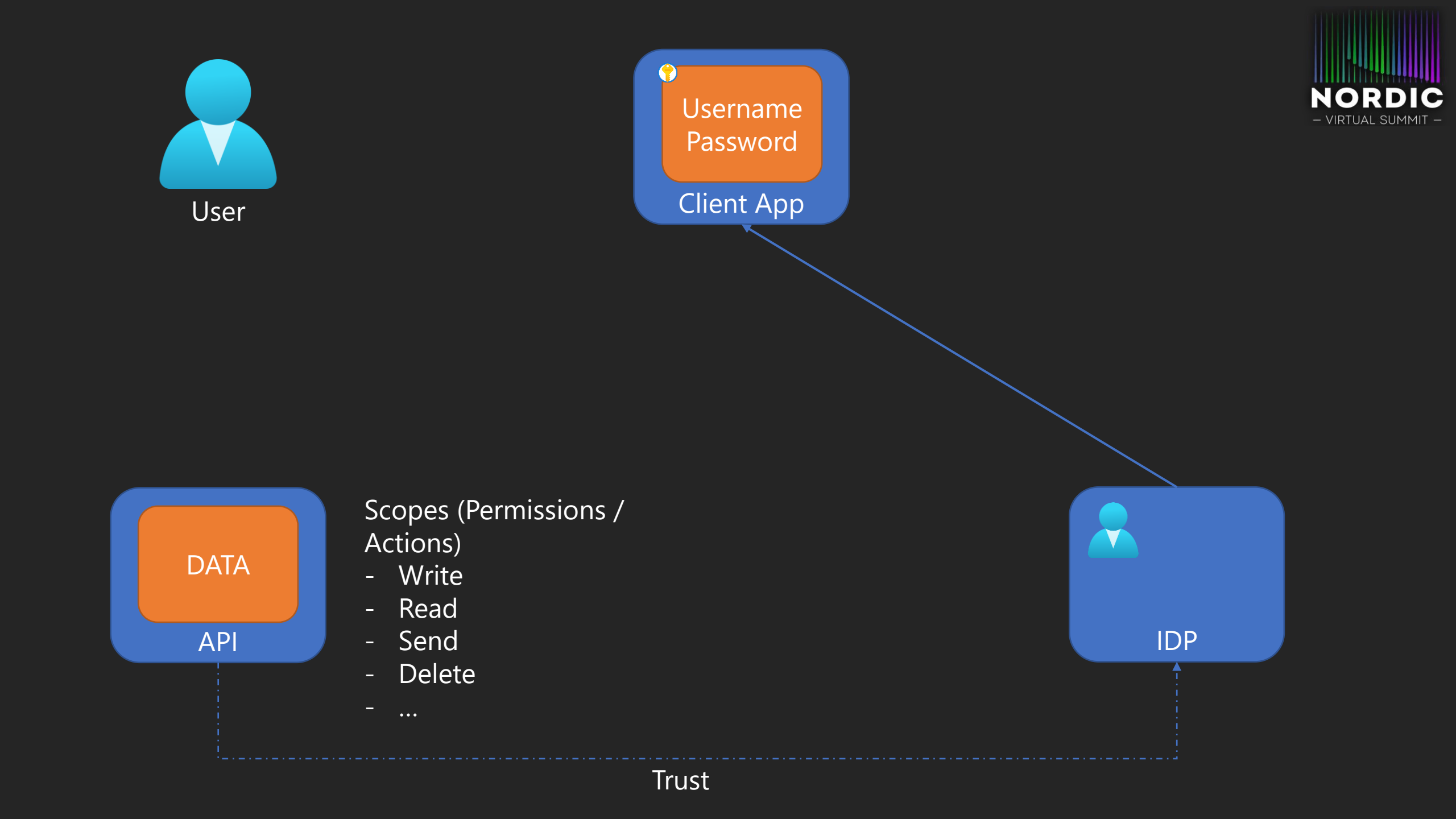
IDP

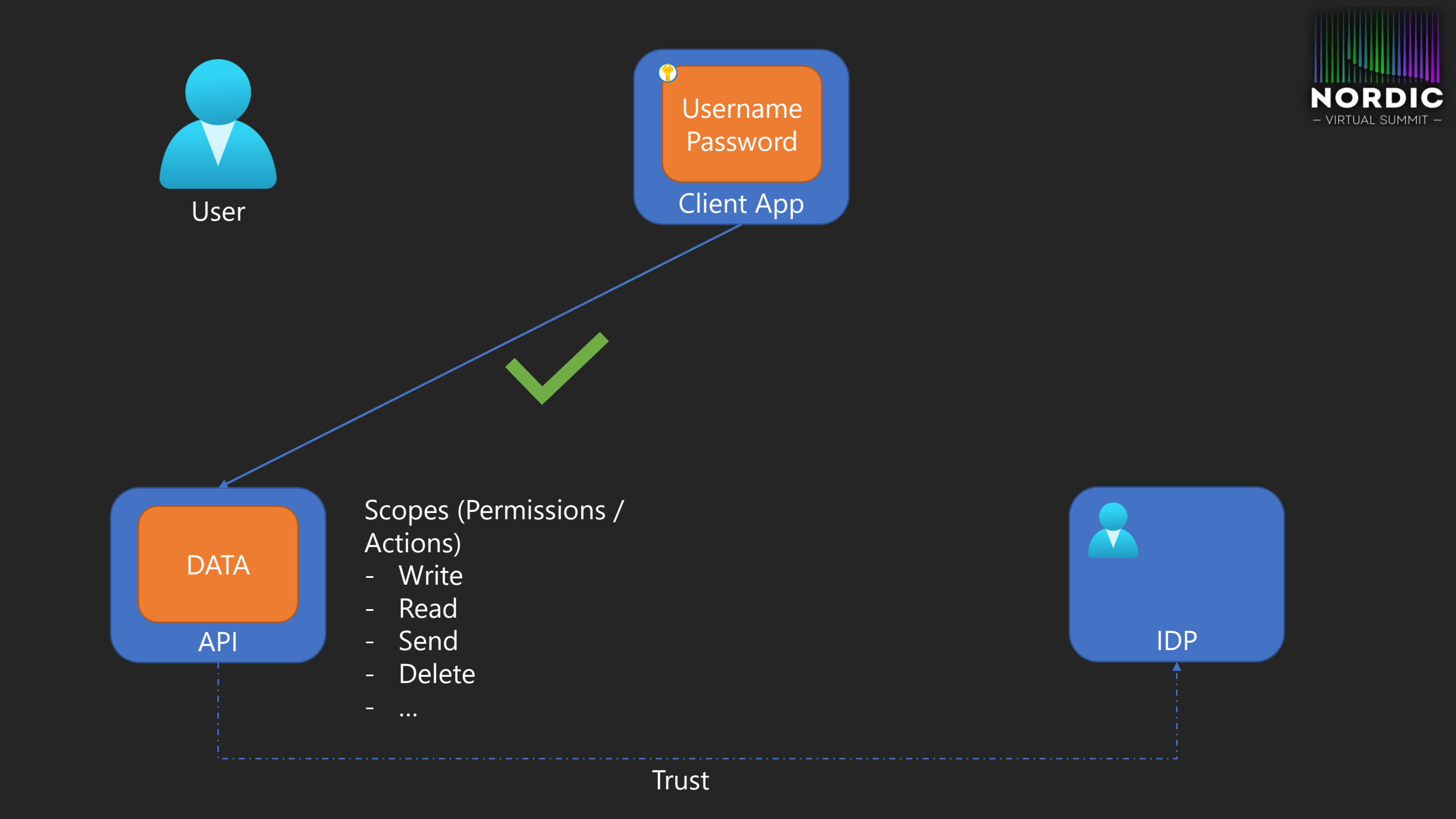
Trust


User
Client App
?
DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
IDP
Trust

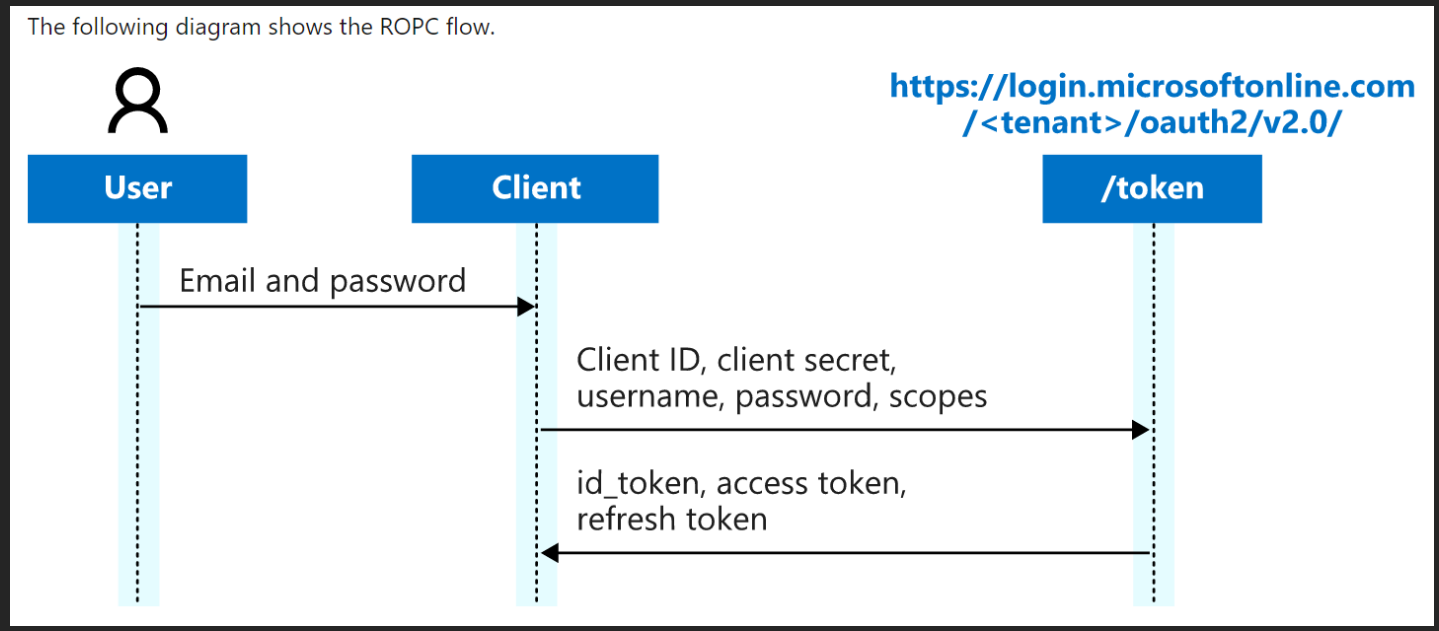

User
Username
Password
Client App
DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
IDP
Trust


User
Username
Password
Client App
DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
IDP
Trust


User
Username
Password
Client App
DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
IDP
Trust


User
Username
Password
Client App
DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
IDP
Trust

This is how it flows … in AAD



How to do it better?

User

Client App

DATA

API

Scopes (Permissions / Actions)

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

IDP

Trust

User

Client App

DATA

API

Scopes (Permissions / Actions)

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

Client App

IDP

Trust

User

Client ID
&
Secret

Client App

DATA

API

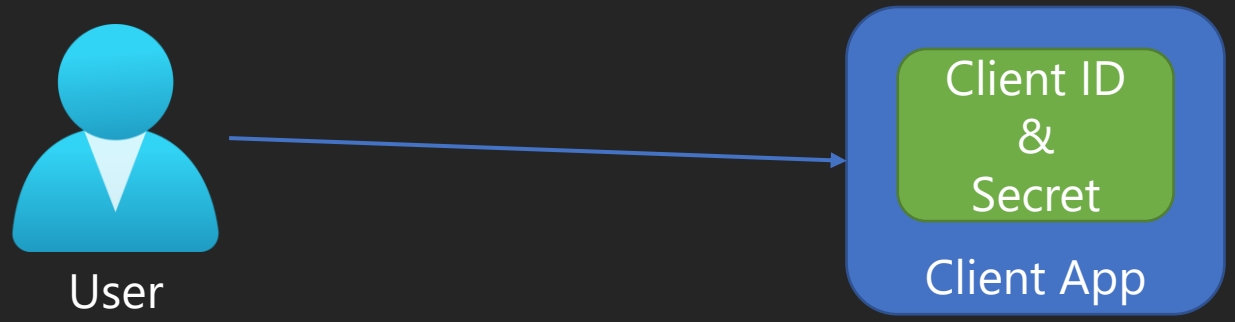
Scopes (Permissions / Actions)

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

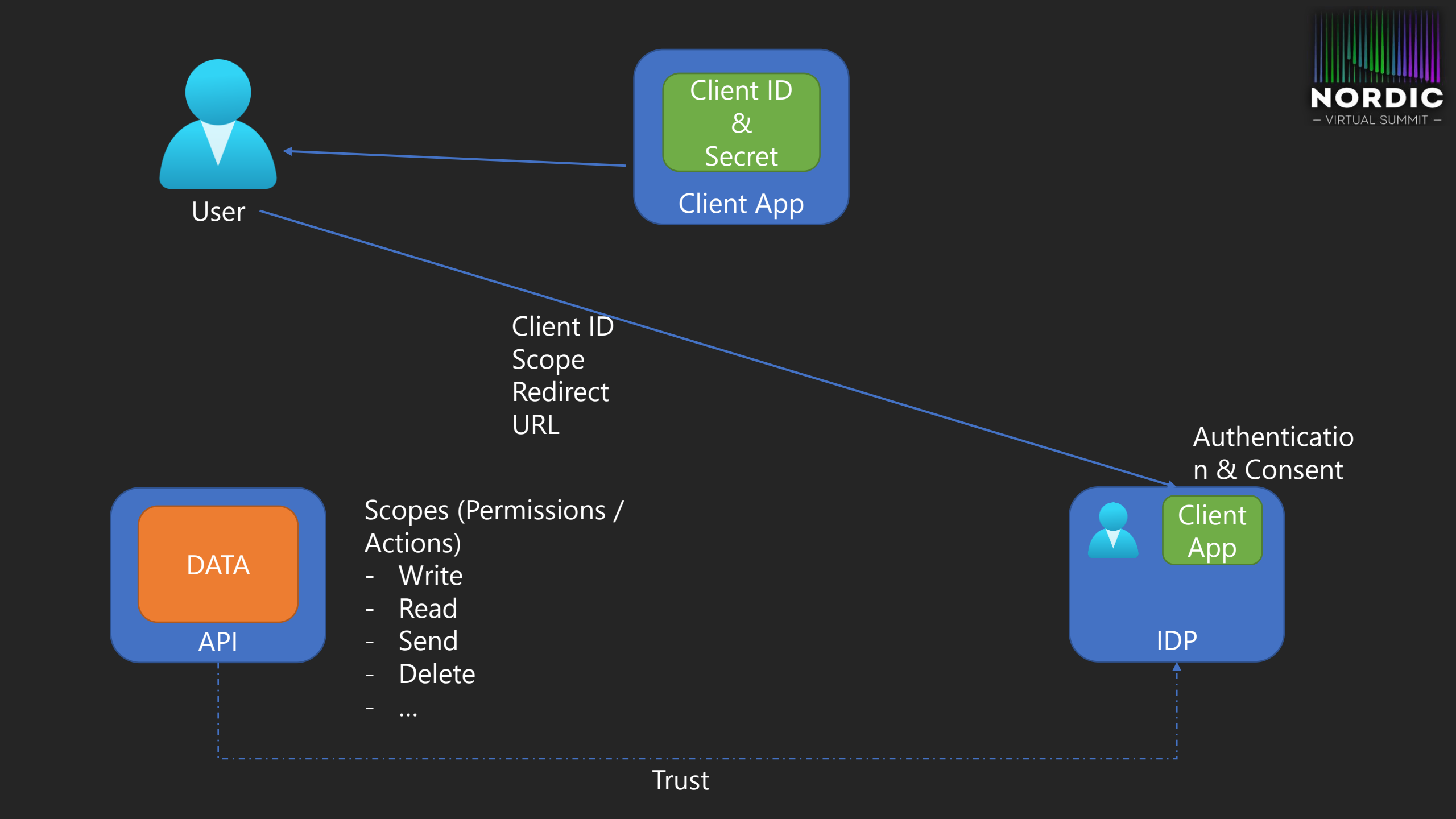
Client App

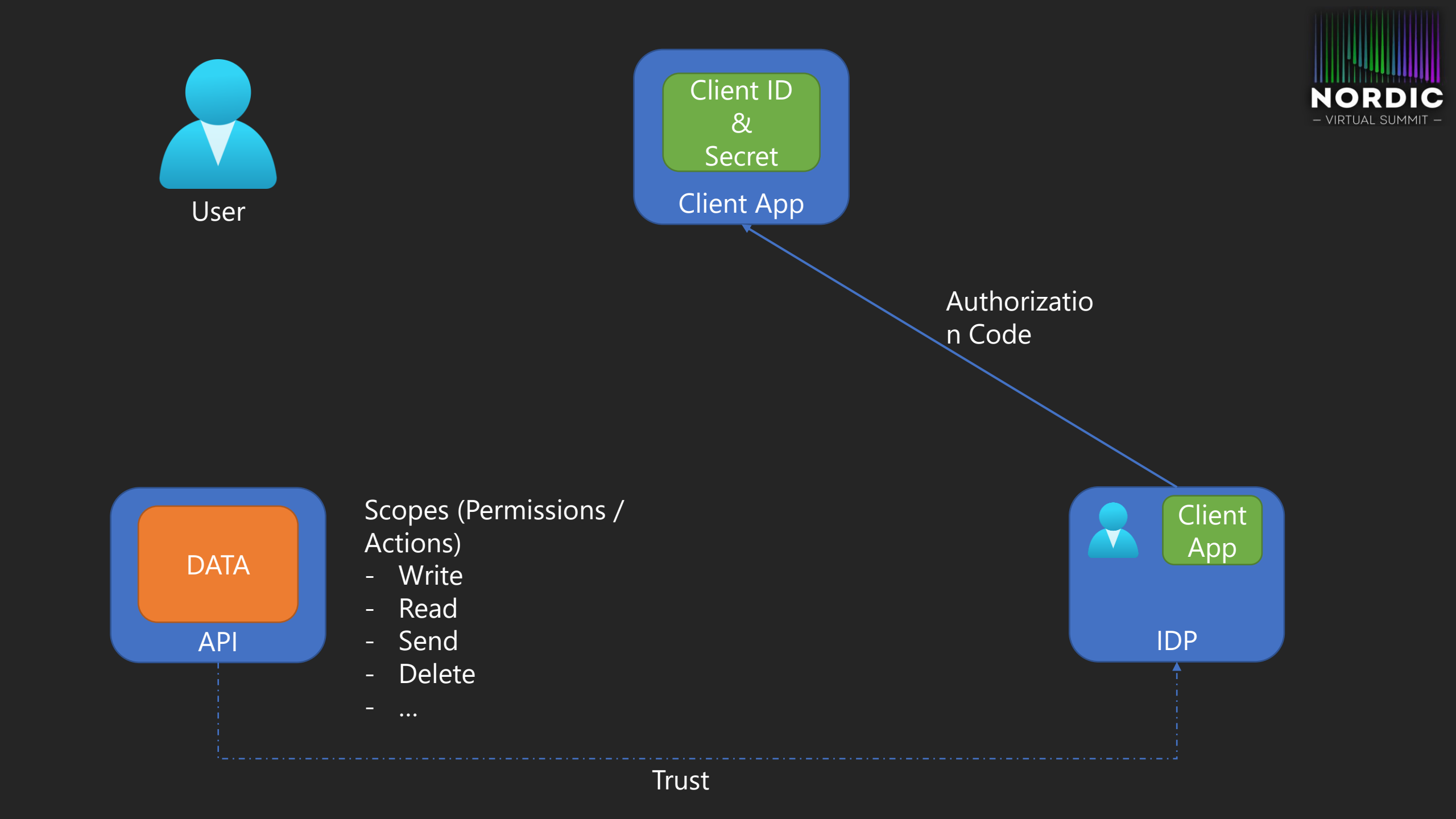
IDP

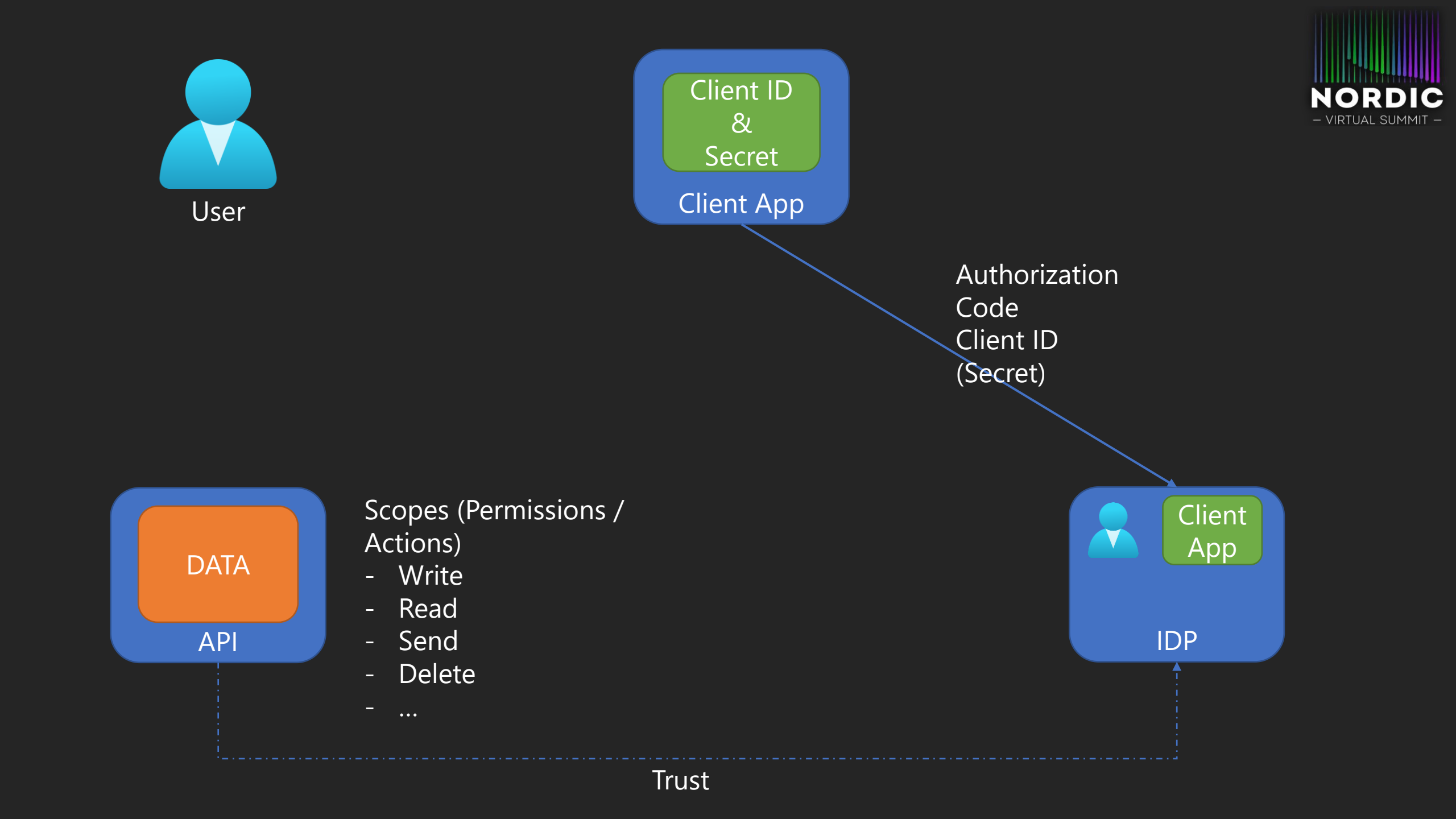
Trust

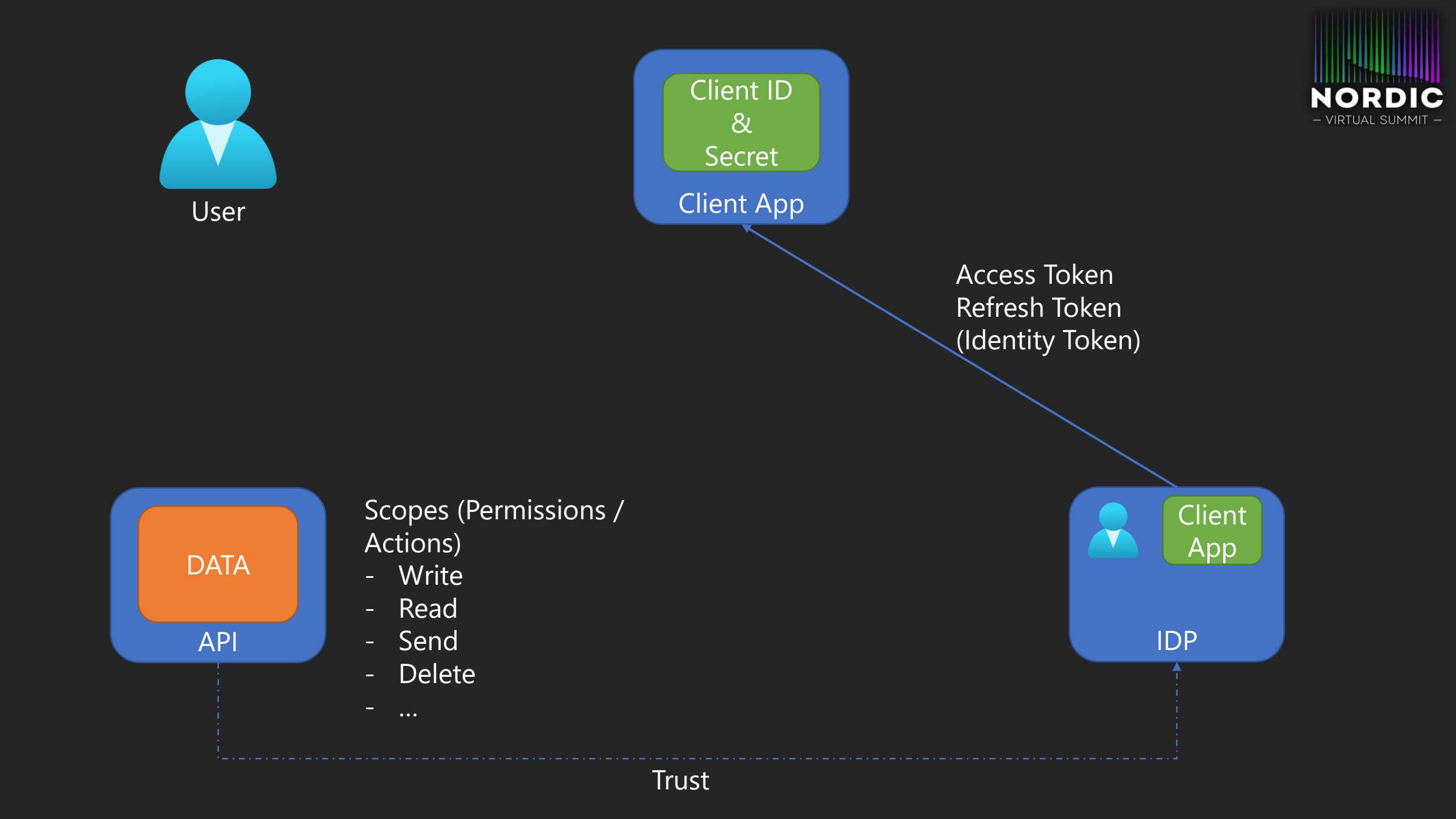

User
Client ID
&
Secret
Client App

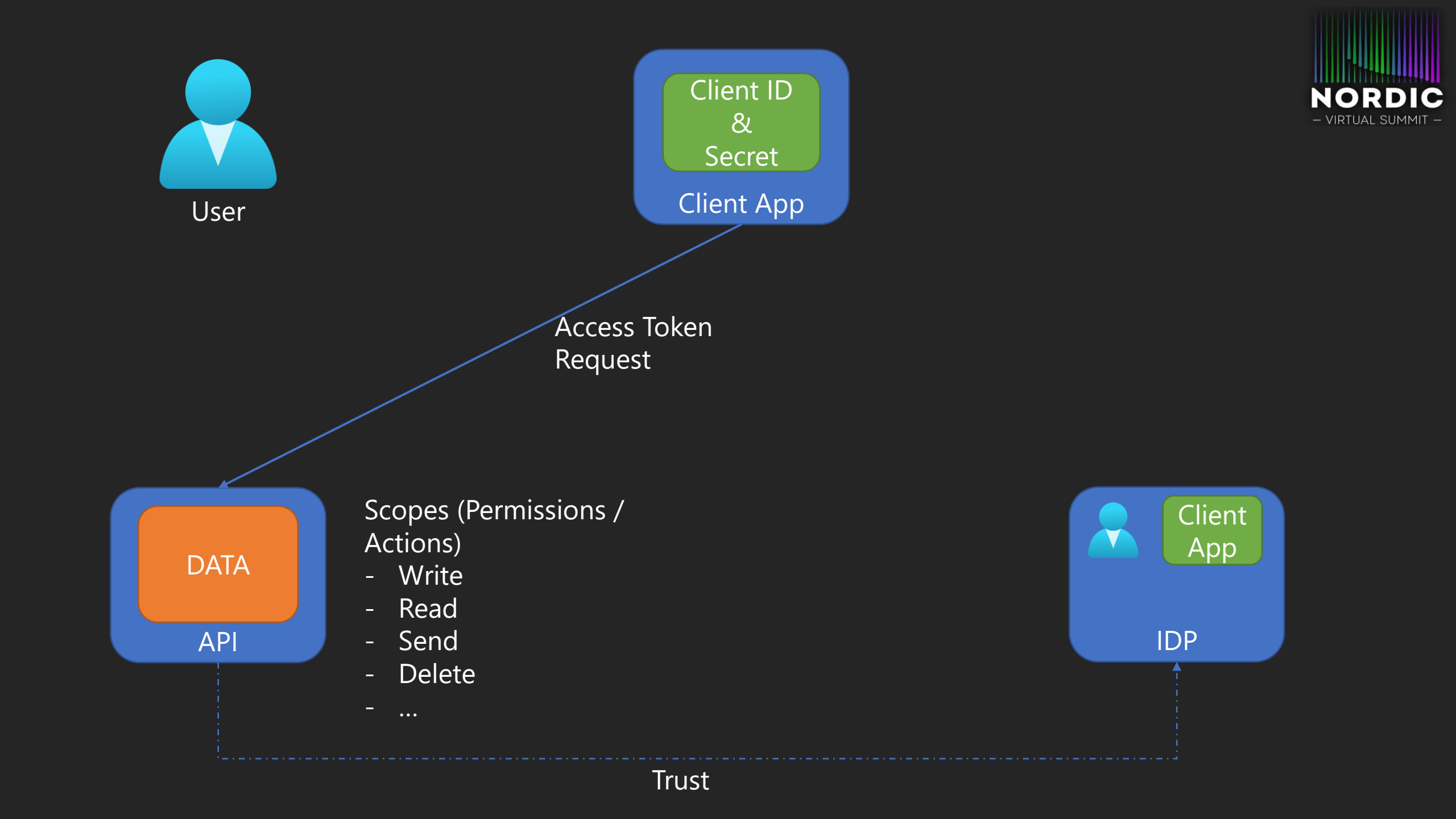

DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
Client App
IDP
Trust

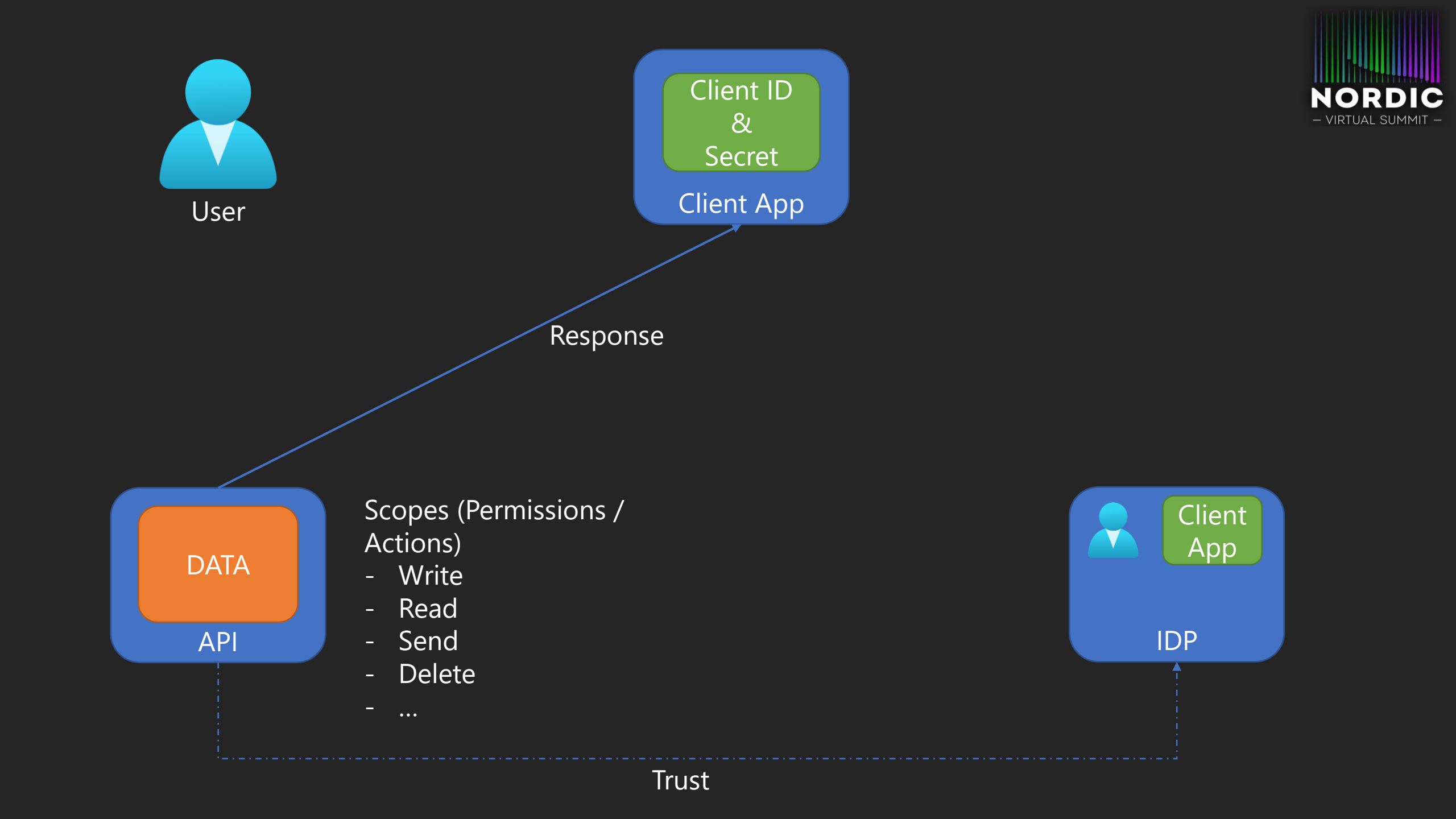

Client ID
&
Secret
Client App
User
Client ID
Scope
Redirect
URL
Authenticatio
n & Consent
DATA
API
Scopes (Permissions /
Actions)
- Write
- Read
- Send
- Delete
- ...
Client
App
IDP
Trust


User
Client ID
&
Secret
Client App
Authorizatio
n Code
DATA
API
Scopes (Permissions /
Actions)
- Write
- Read
- Send
- Delete
- ...
Client
App
IDP
Trust

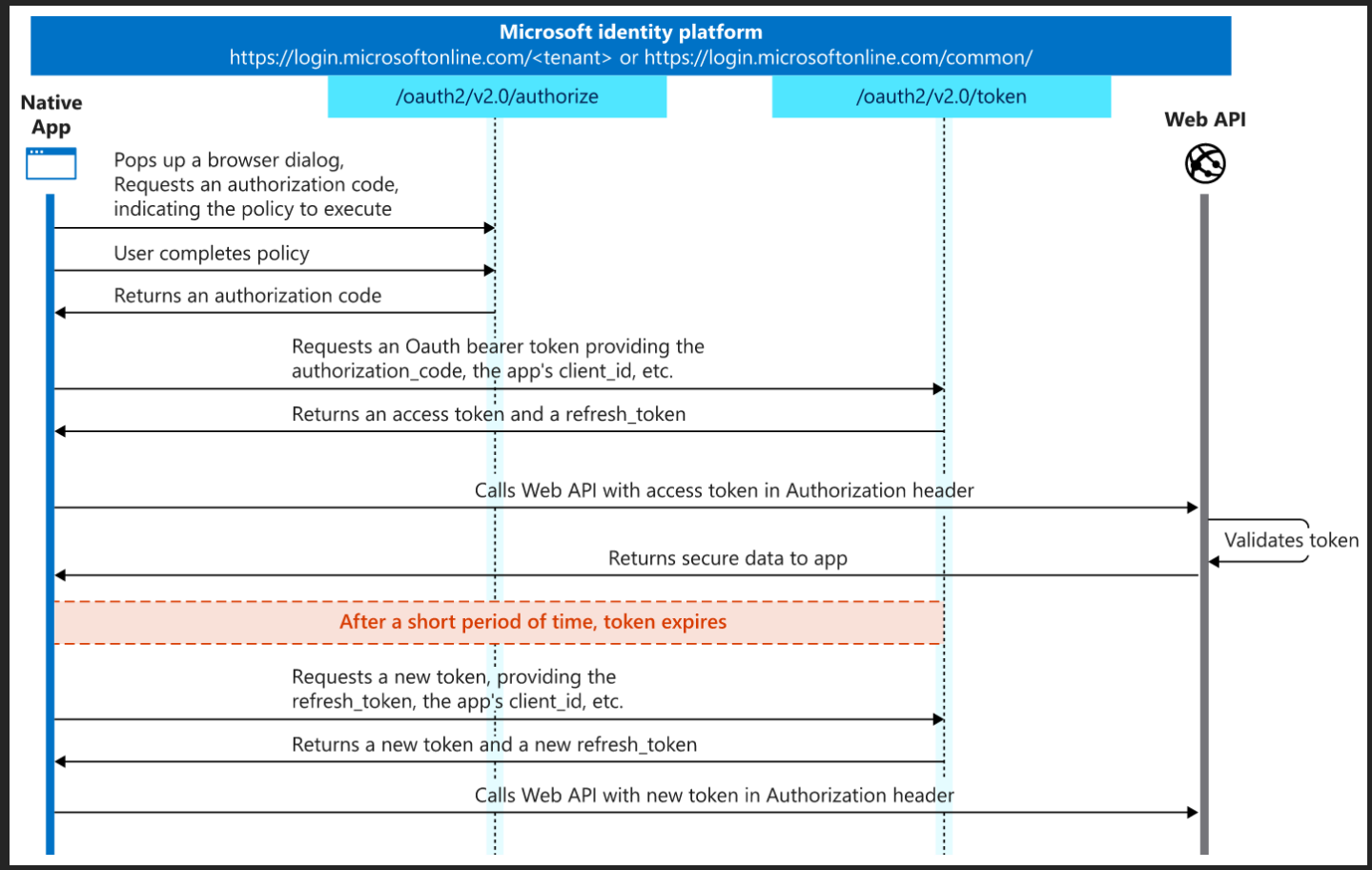

User
Client ID
&
Secret
Client App
Authorization
Code
Client ID
(Secret)
DATA
API
Scopes (Permissions /
Actions)
- Write
- Read
- Send
- Delete
- ...
Client
App
IDP
Trust


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


User
Client ID
&
Secret
Client App
Response
DATA
API
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- ...
Client App
IDP
Trust

This is how it flows … in AAD



And what about AAD now?

User

Client App

DATA

API

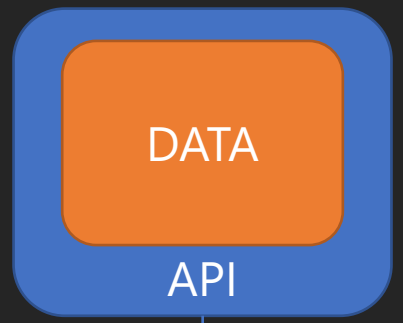
Scopes (Permissions / Actions)

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

IDP

Trust

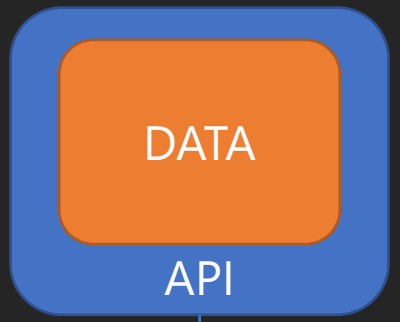
User



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

Trust

User



Scopes (Permissions / Actions)

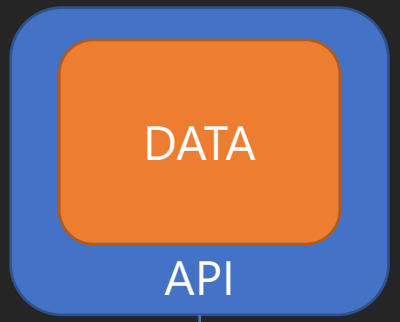
- Write
- Read
- Send
- Delete
- …

Azure AD

Trust

User

App Registration
Unique ID
Scope
Secret



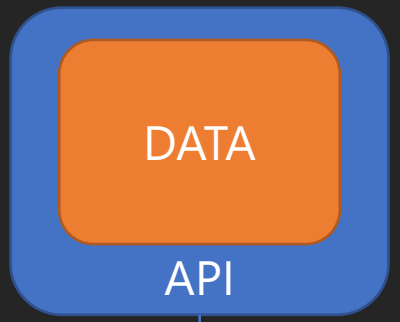
Scopes (Permissions / Actions)
- Write
- Read
- Send
- Delete
- …

Azure AD

Trust

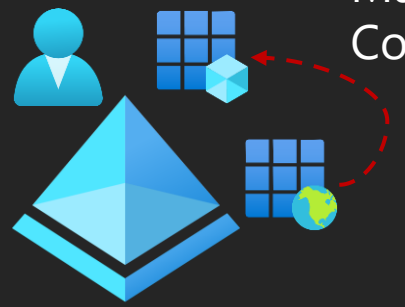
DEMO?!

User



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

Service Principal Management Consent



Azure AD

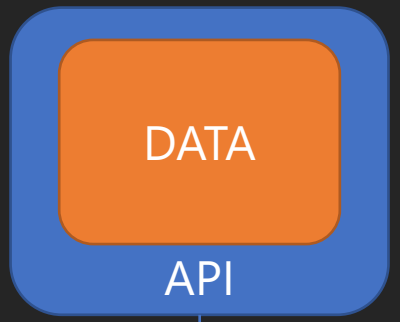
Trust

DEMO?!

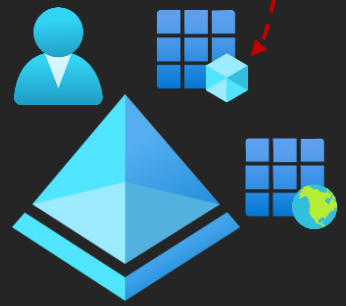
User

Service Principal Management Consent

Azure AD 2



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



Azure AD

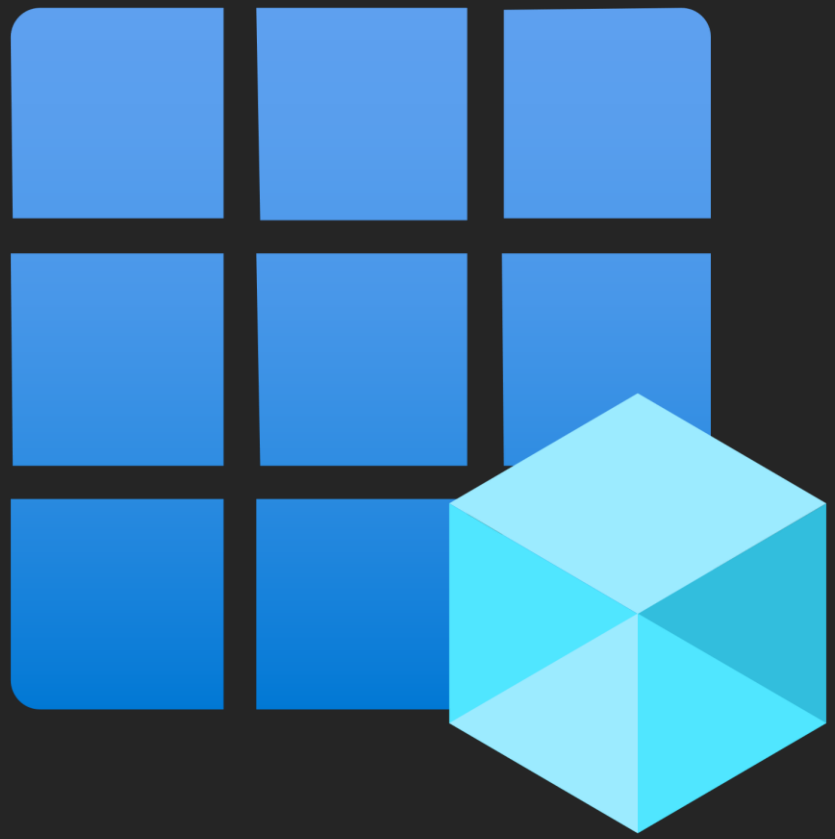
Trust

NORDIC
– VIRTUAL SUMMIT –

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

A big thanks to our sponsors

NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

Thank you!

NORDIC
– VIRTUAL SUMMIT –

Please remember to fill out the evals!

https://stream.nordicvirtualsummit.com/feedback