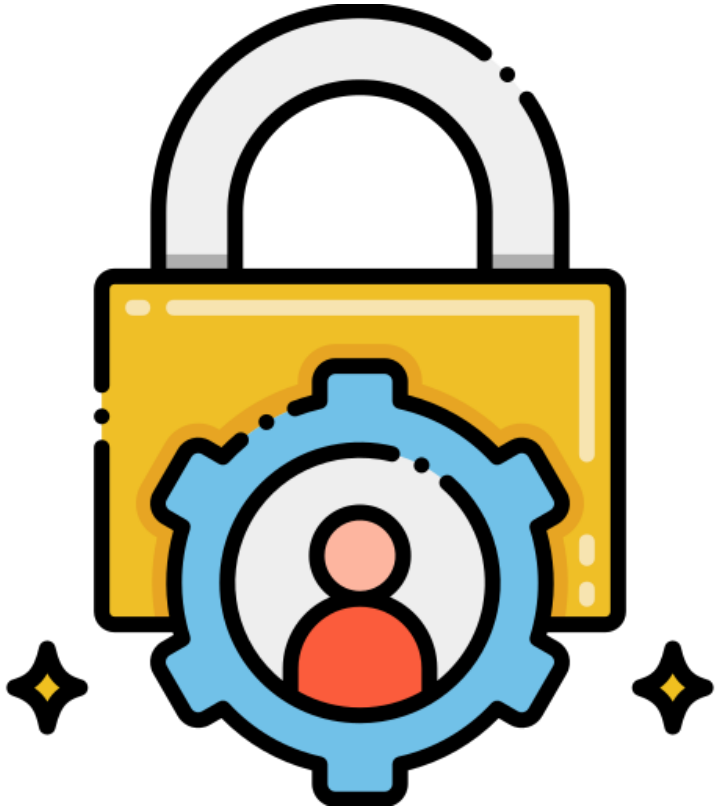
Representing Application Permissions Models via the SCIM 2.0 Roles and Entitlements Attributes

Danny Zollner

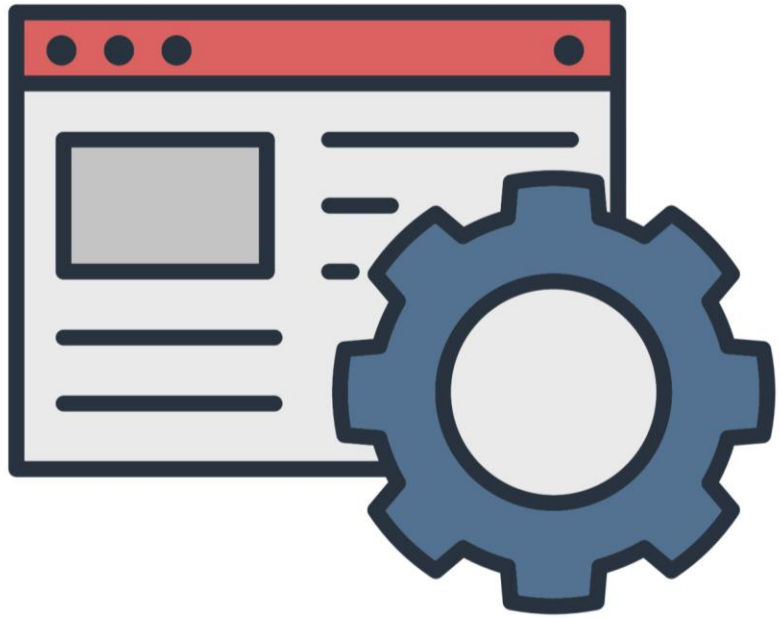
Senior Product Manager

Microsoft

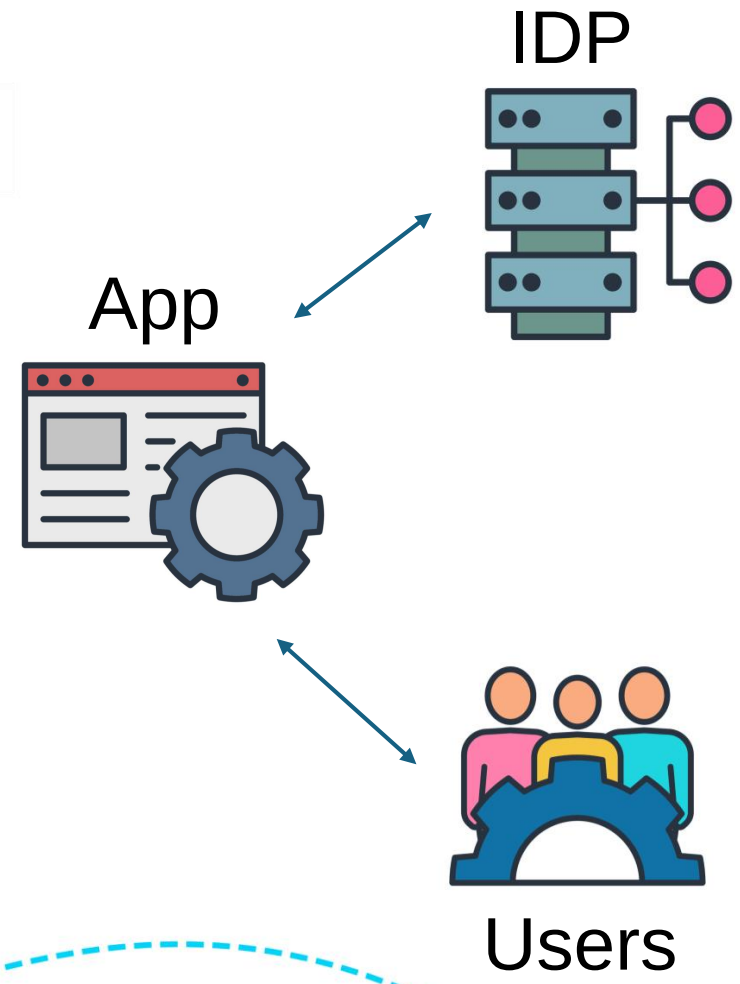


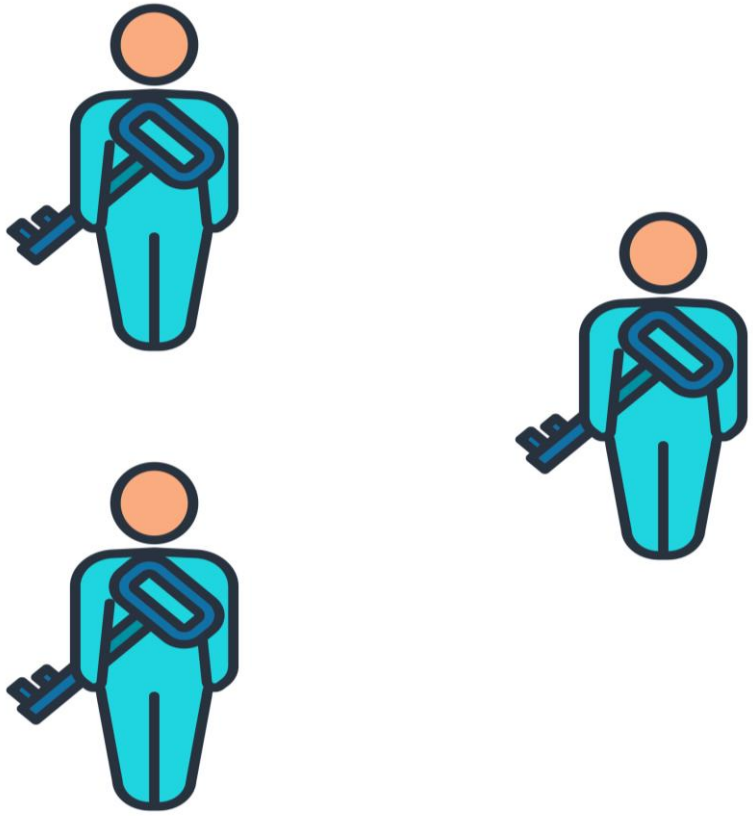
Introduction

- Most organizations have applications connected to an IdP
- SCIM allows for provisioning identity data into applications
- Applications have permission models
- Most applications with SCIM don’t represent permissions beyond very coarse-grained roles at best

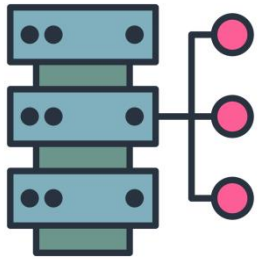


Wild Permissions Appeared!

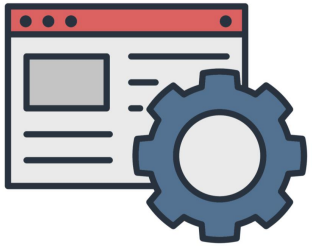




IDP

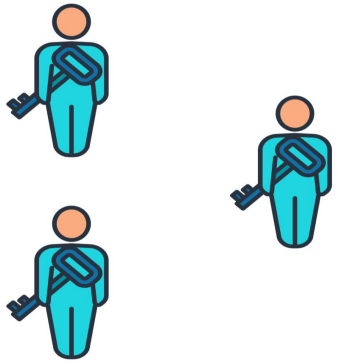


App



Users

Permissions



IDP

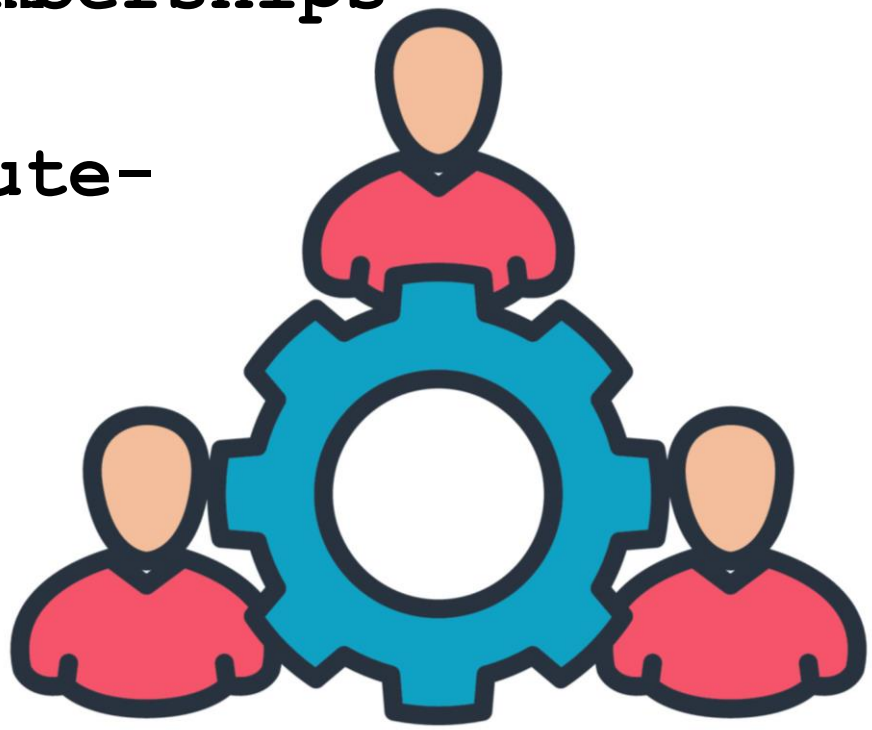
App

Users

Permissions

Group Memberships

Attribute-based



IDP

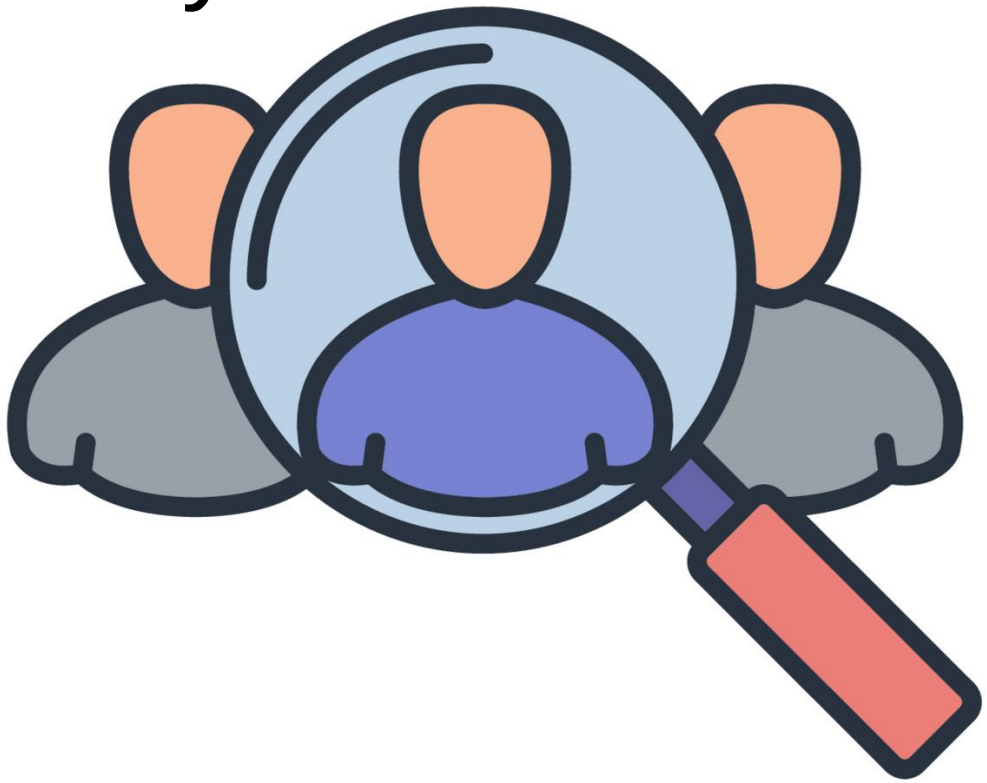
App

Users

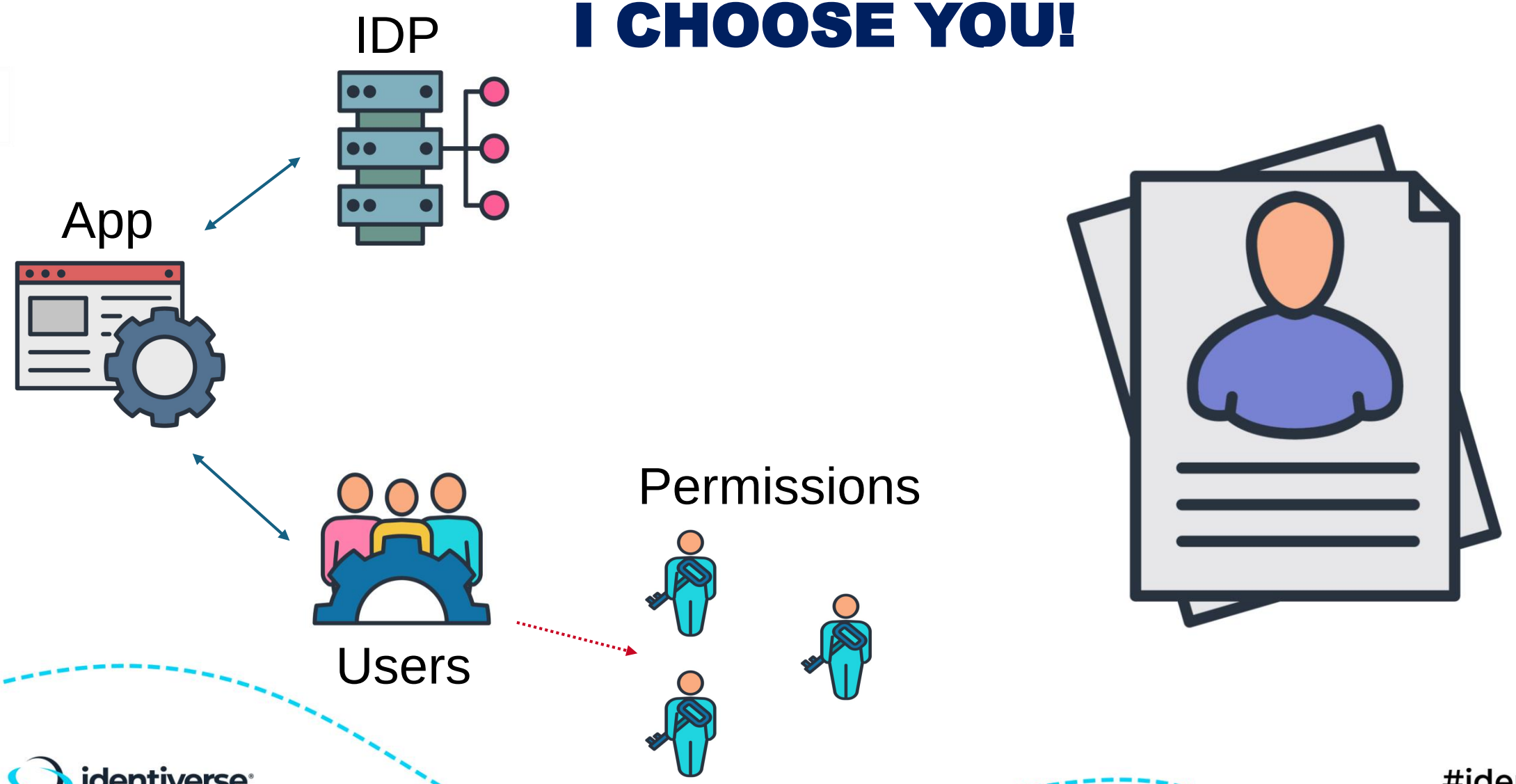
Permissions

Visibility

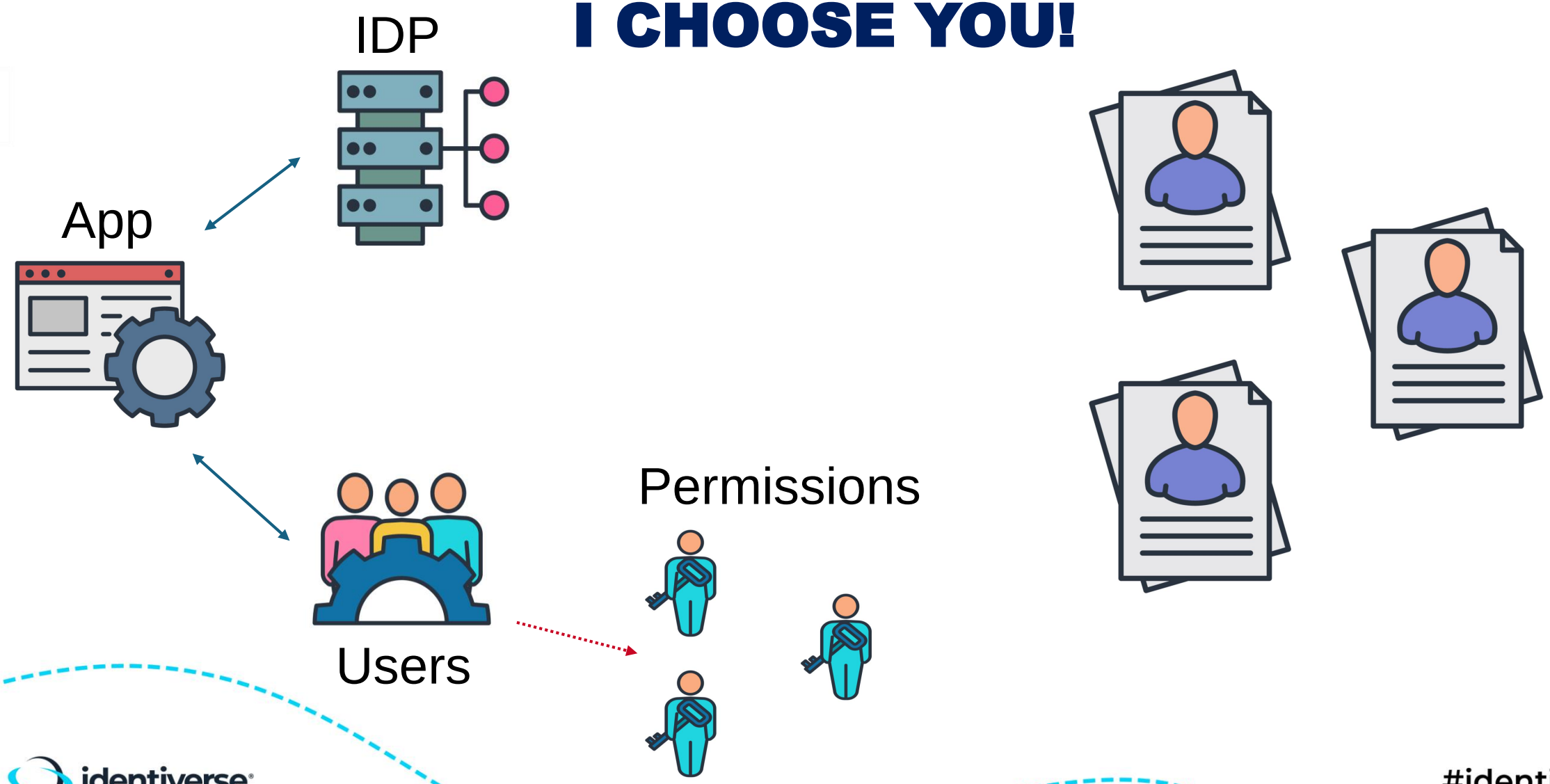
Control

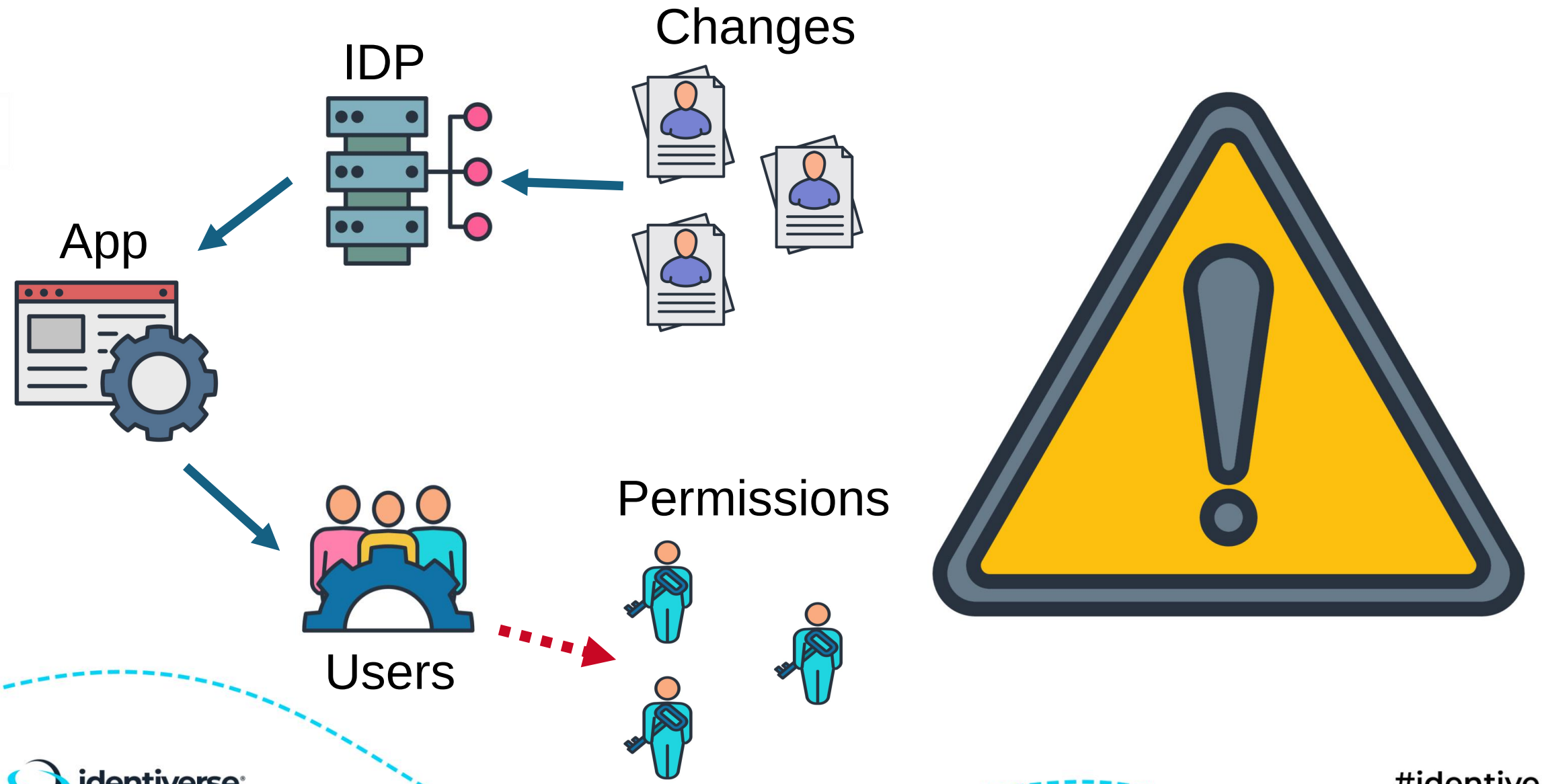


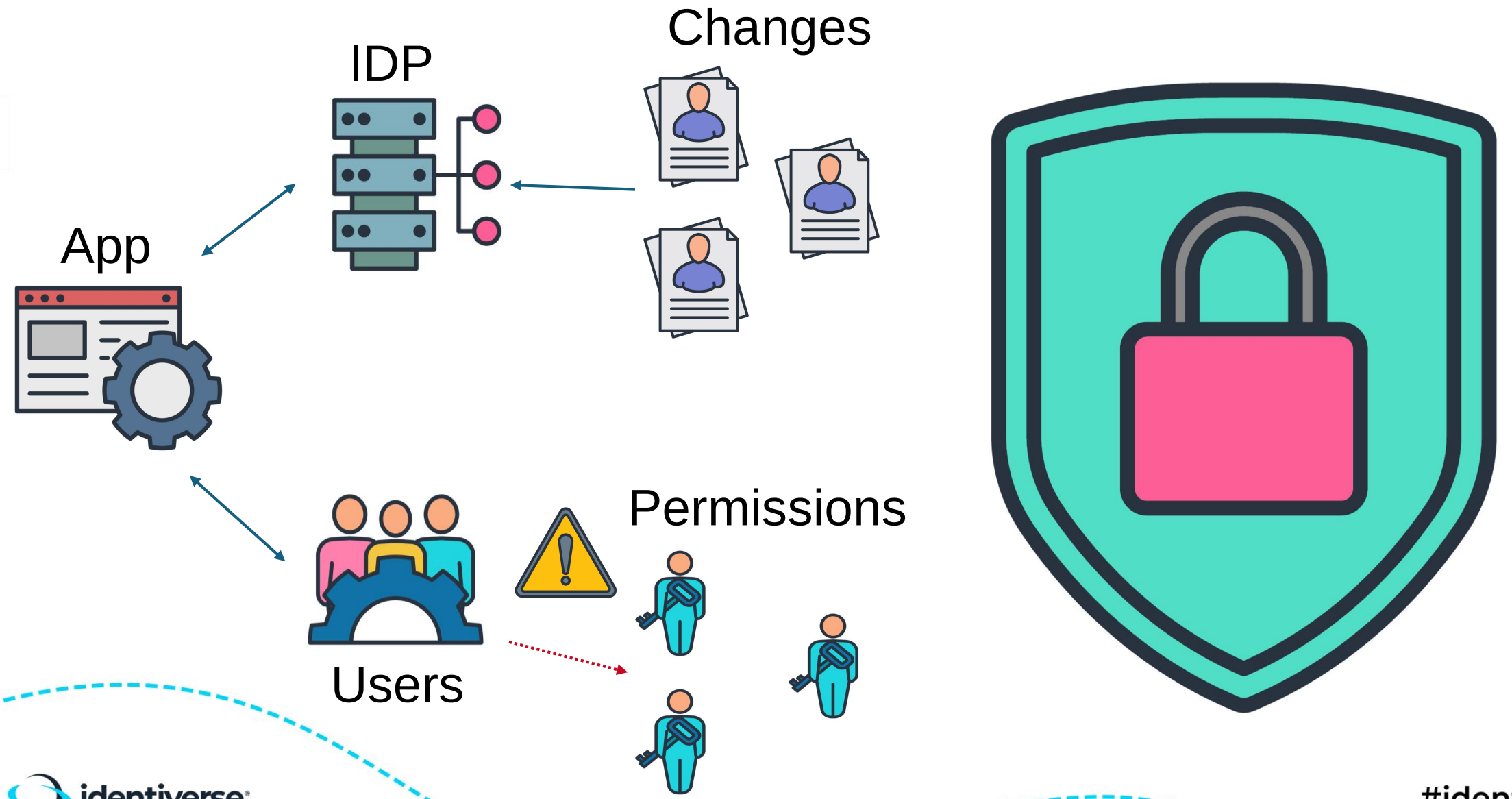
HR System as the Source of Truth, GO!
I CHOOSE YOU!

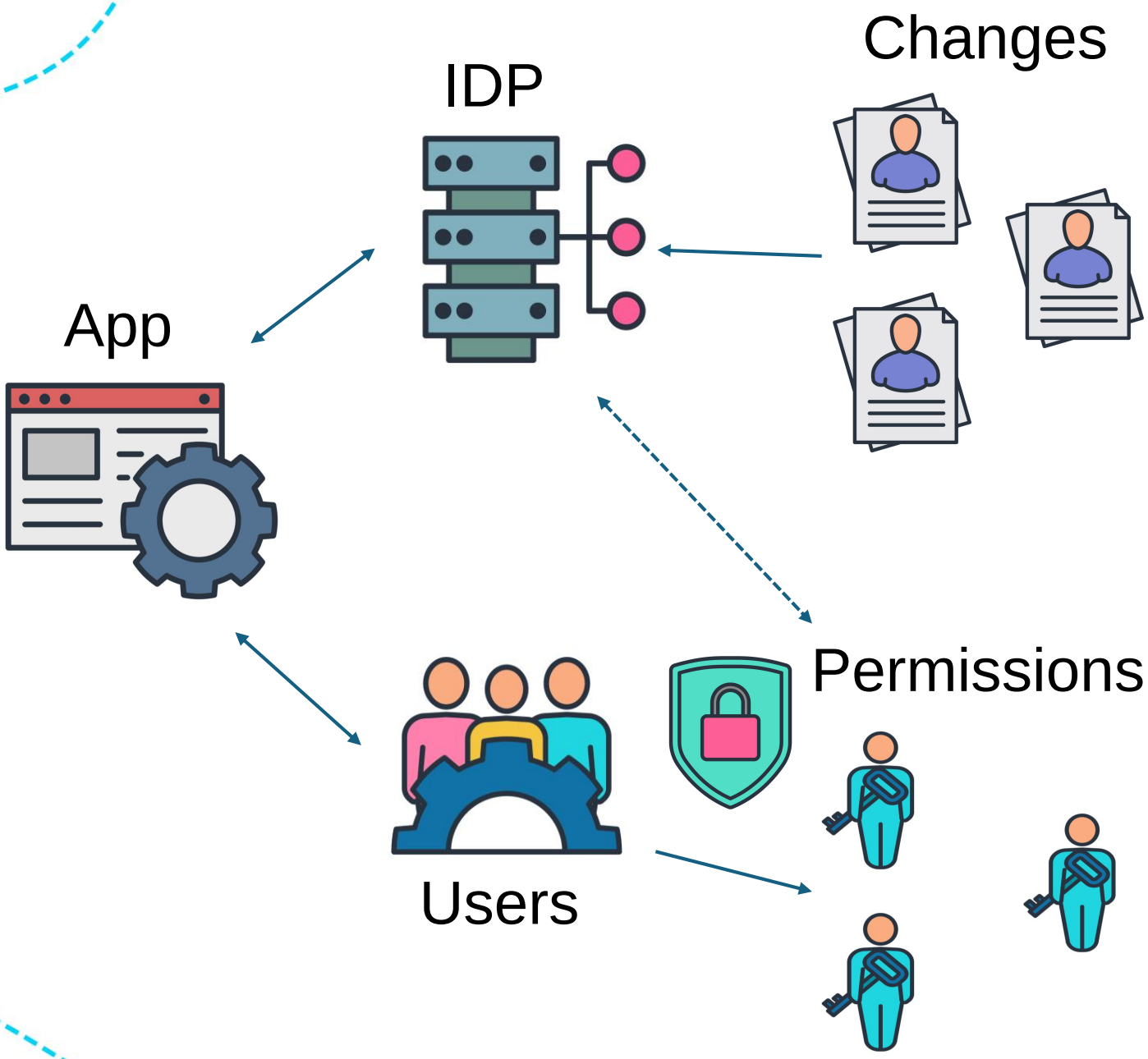


HR System as the Source of Truth, GO!
I CHOOSE YOU!

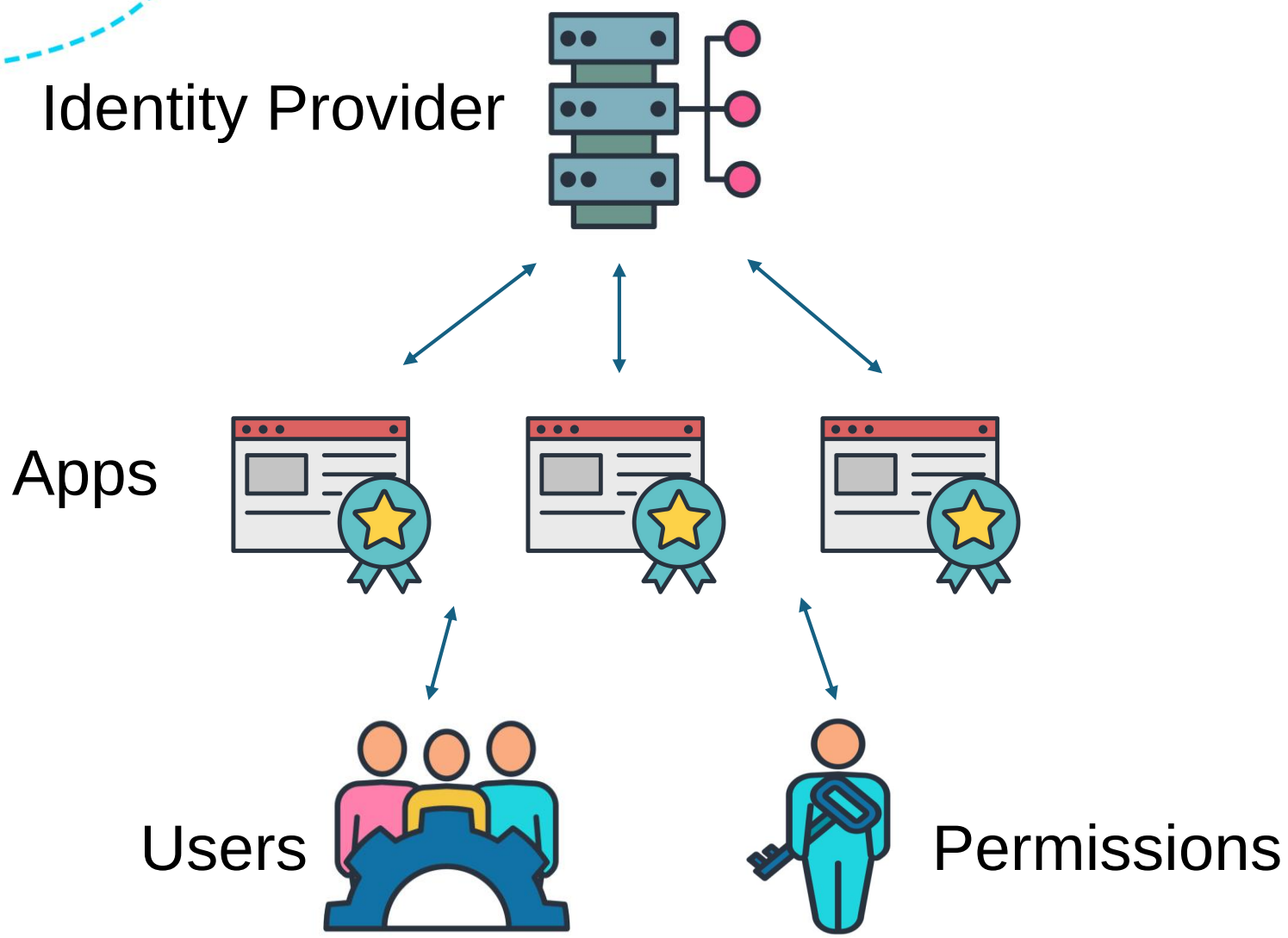


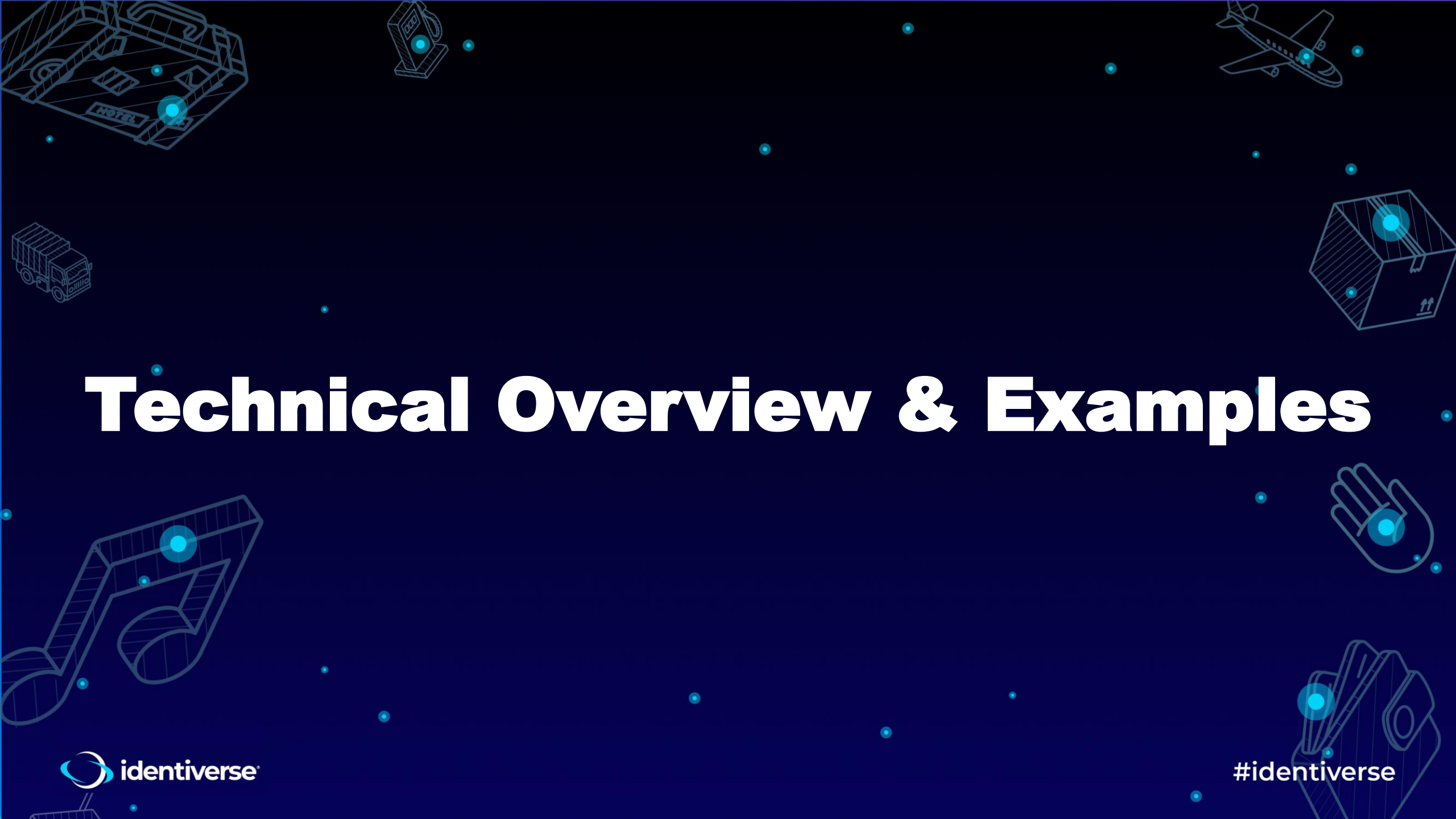

Changes
IDP
App
Permissions
Users


Changes
IDP
App
Permissions
Users


Changes
IDP
App
Permissions
Users

Identity
Provider


Identity Provider
Apps
Users
Permissions



Technical Overview & Examples

How are permissions represented in SCIM?

How are permissions represented in SCIM?

Complex + multi-valued attributes on the core user schema

Sub-attributes:

- display
- value
- type
- primary

Entitlements

A list of entitlements for the user that represent a thing the user has. An entitlement may be an additional right to a thing, object, or service.

Roles

A list of roles for the user that collectively represent who the user is, e.g., "Student", "Faculty". ..it is expected that a role value is a String or label representing a collection of entitlements.

Sub-attribute JSON Example

```
“roles” / “entitlements”:[
{
“display”:”Administrator”,
“value”:”admin”,
“type”:”Global”,
“primary”:false
}
]
```

Example roles

ADMINISTRATOR

Display

Human Readable Name

Administrator

Value

Identifier in underlying system

admin

Type

Organizational Label

Global

Primary

Primary / Secondary Indicator

False

Example roles

ADMINISTRATOR

Display

Administrator

Value

18fb029c-1502-4497-aa73-6ea0b47b7626

Type

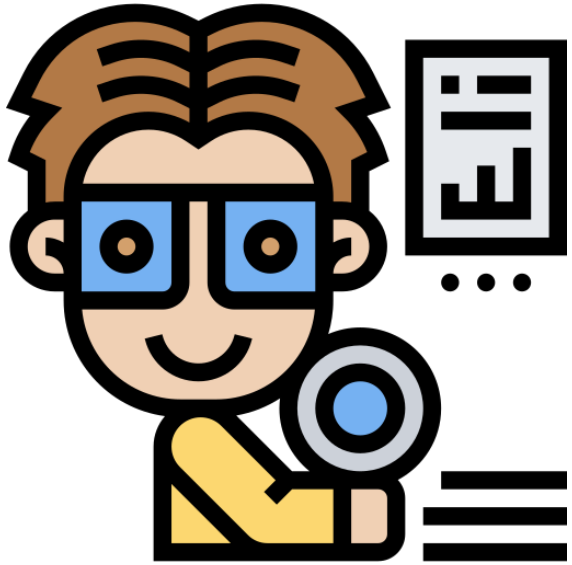
CRM_App

Primary

False

Example roles

AUDITOR



Display

Auditor

Value

Auditor

Type

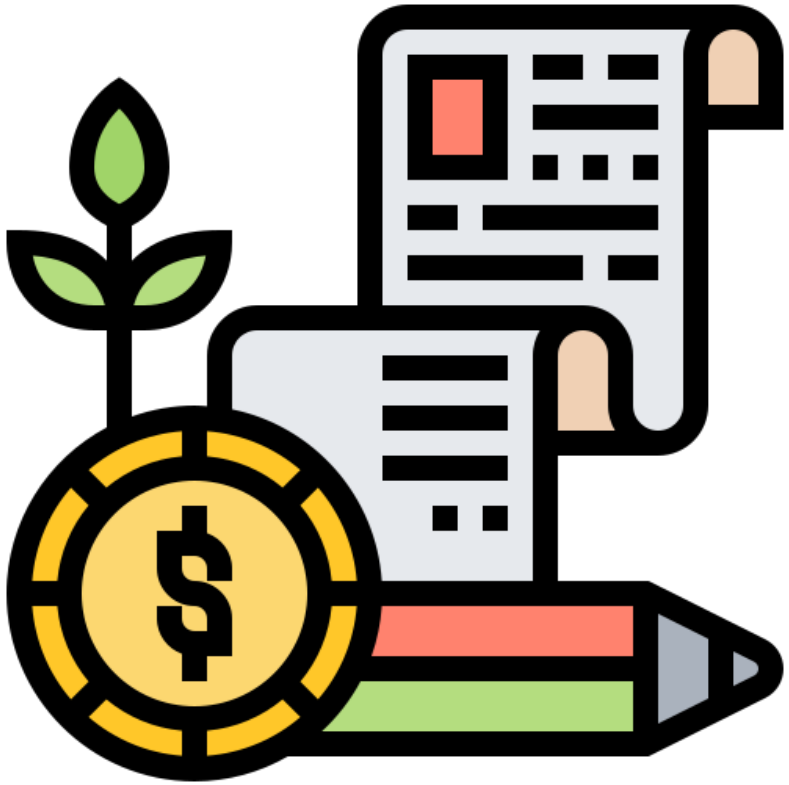
FooSoft App

Primary

True

Example roles

ACCOUNTING



Display

Accounting

Value

Accounting

Type

FooSoft App

Primary

False

Example roles

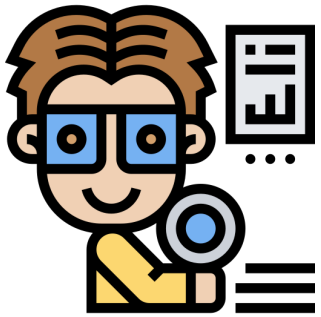
AUDITOR

Display
Auditor

Value
Auditor

Type
FooSoft App

Primary
True



ACCOUNTING

Display
Accounting

Value
Accounting

Type
FooSoft App

Primary
False

ROLES + ENTITLEMENTS

Example

ROLES

Display

App Full Access

Value

App_Full

ENTITLEMENTS

Display

App Read Access

Value

App_Read

Display

App Write Access

Value

App_Write

Display

App Delete Access

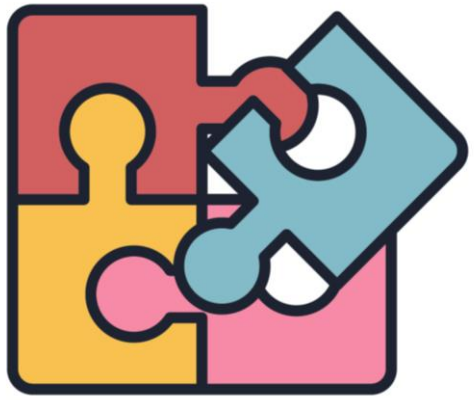
Value

App_Delete

Upcoming Work

Current Problems

Not all values are valid



Lack of discoverability

Each app is different

Proposed Solution – SCIM

New SCIM draft – SCIM Roles and Entitlements Extension

https://dt.ietf.org/doc/draft-ietf-scim-roles-entitlements/

SCIM D. Zollner
Internet-Draft Microsoft
Intended status: Standards Track 7 December 2022
Expires: 10 June 2023

SCIM Roles and Entitlements Extension
draft-ietf-scim-roles-entitlements-00

What does the draft add?

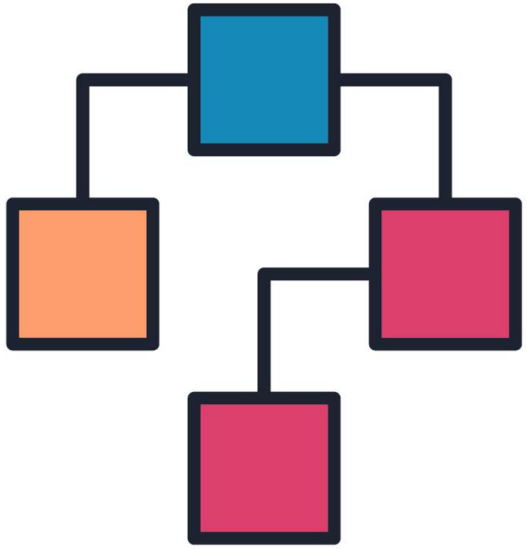
- Read-only /roles and /entitlements endpoints
- /ServiceProviderConfig entries
- /roles and /entitlements include attributes that show:
  - Relationships between permissions
  - Requirements and limits on permission assignments

Requirements and Relationships

Limited Assignments

Requires / Prohibited With

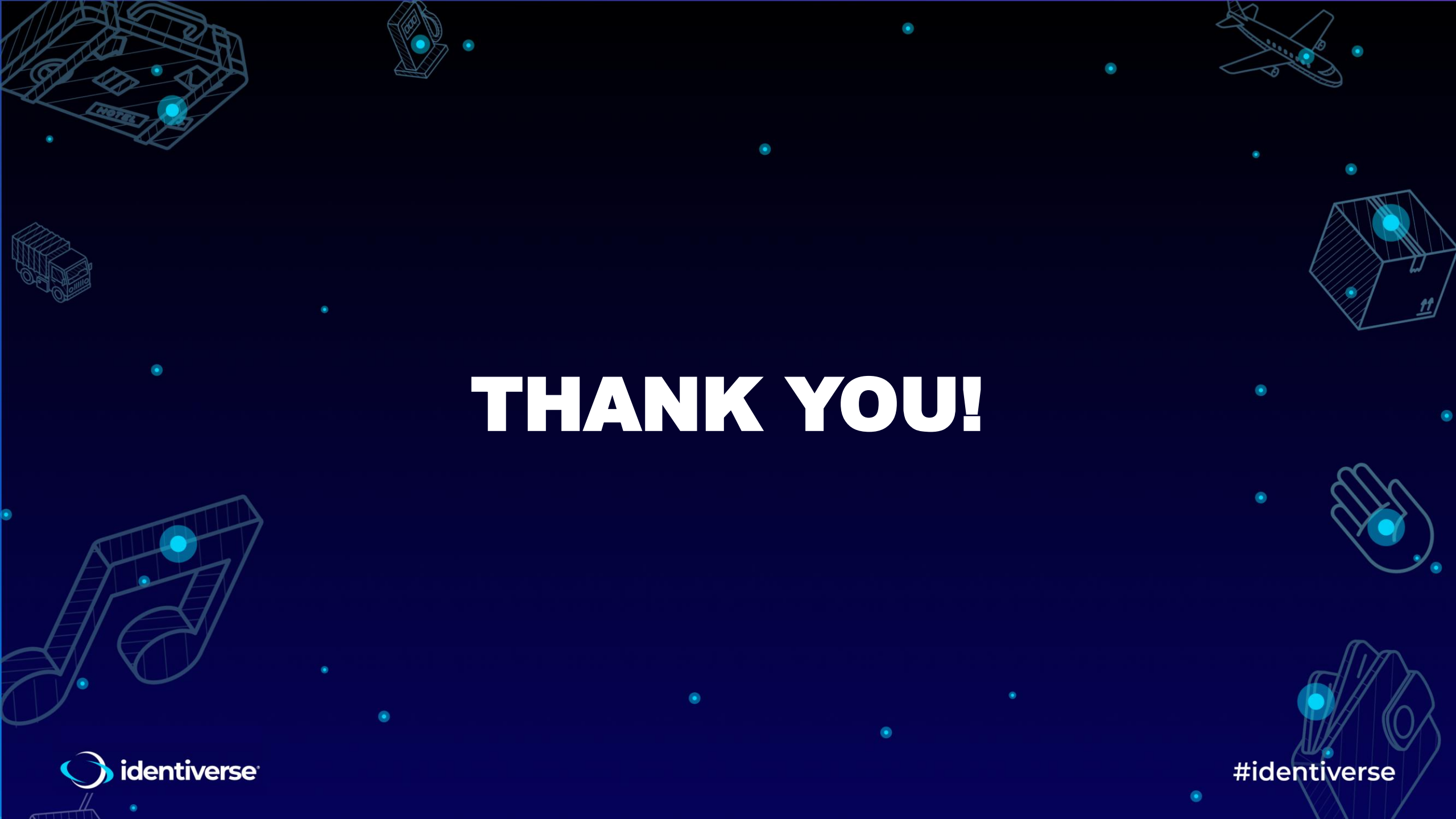
Contains + Contained By



Closing Thoughts

- Representing app permissions in SCIM allows for visibility and centralized management
- Get involved in the standards process! Participate in the IETF SCIM Working Group!

Feedback is CRITICAL!


THANK YOU!
identiverse
#identiverse