WSO2 IDENTITY SERVER

# User Management

# Why User Management

- To securely and efficiently manage user identities
- To define and manage access rights
- To grant the necessary access rights to users based on their authority

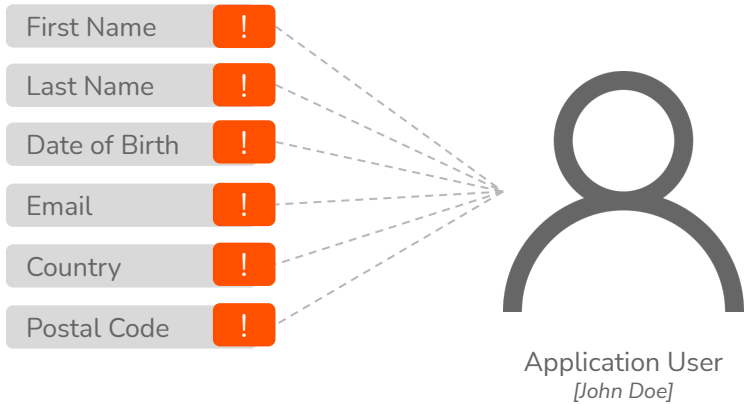
# Users and Claims

# User

The digital representation of a physical user who interacts with an application

# User Claims

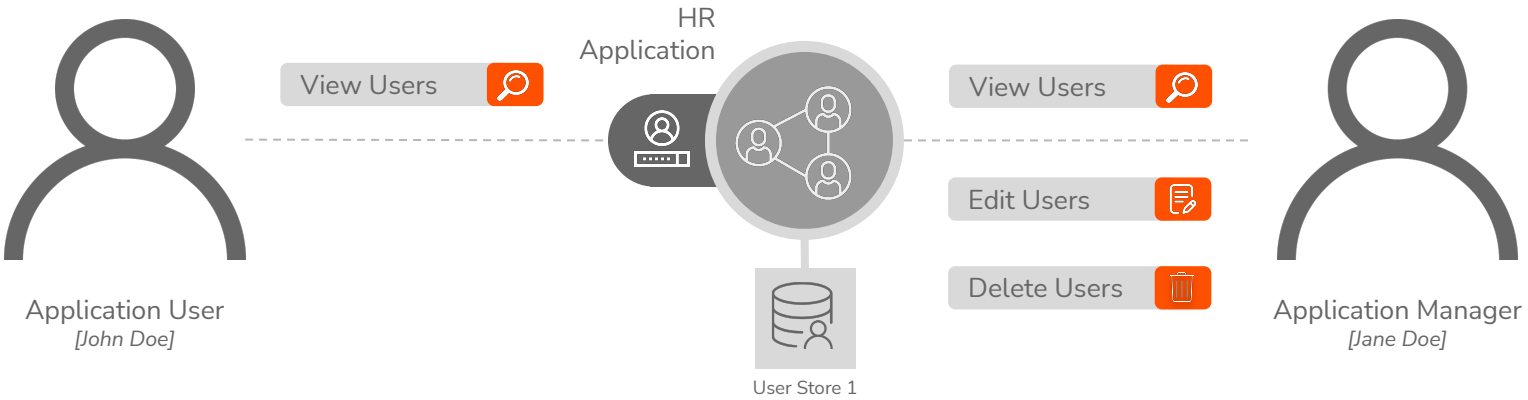
Data that defines the user, i.e., anything the user is, owned by, and associated with



# Permissions and Roles

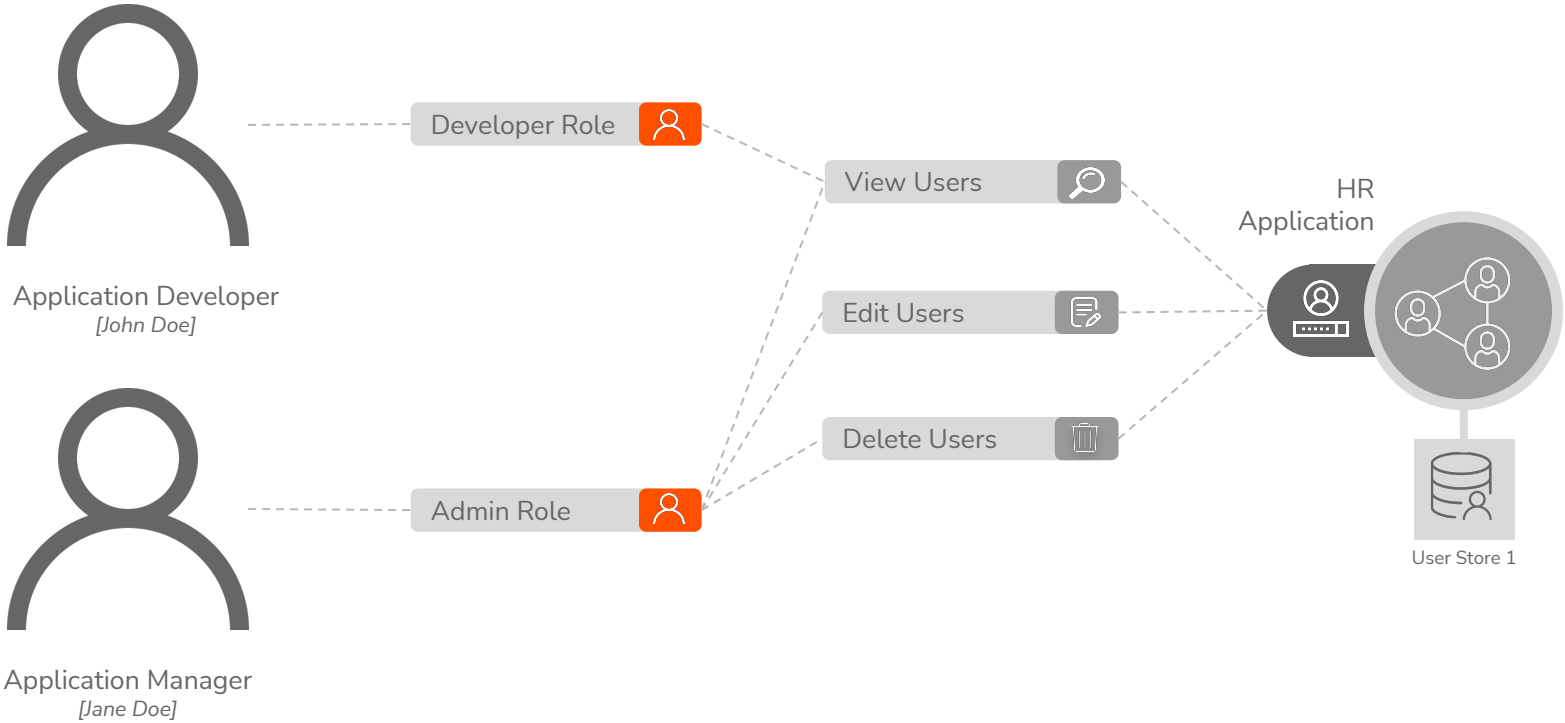
# Permissions

The actions the users are authorized to perform



# User Roles

A group of permissions that can be assigned to users depending on their job profile, e.g., manager



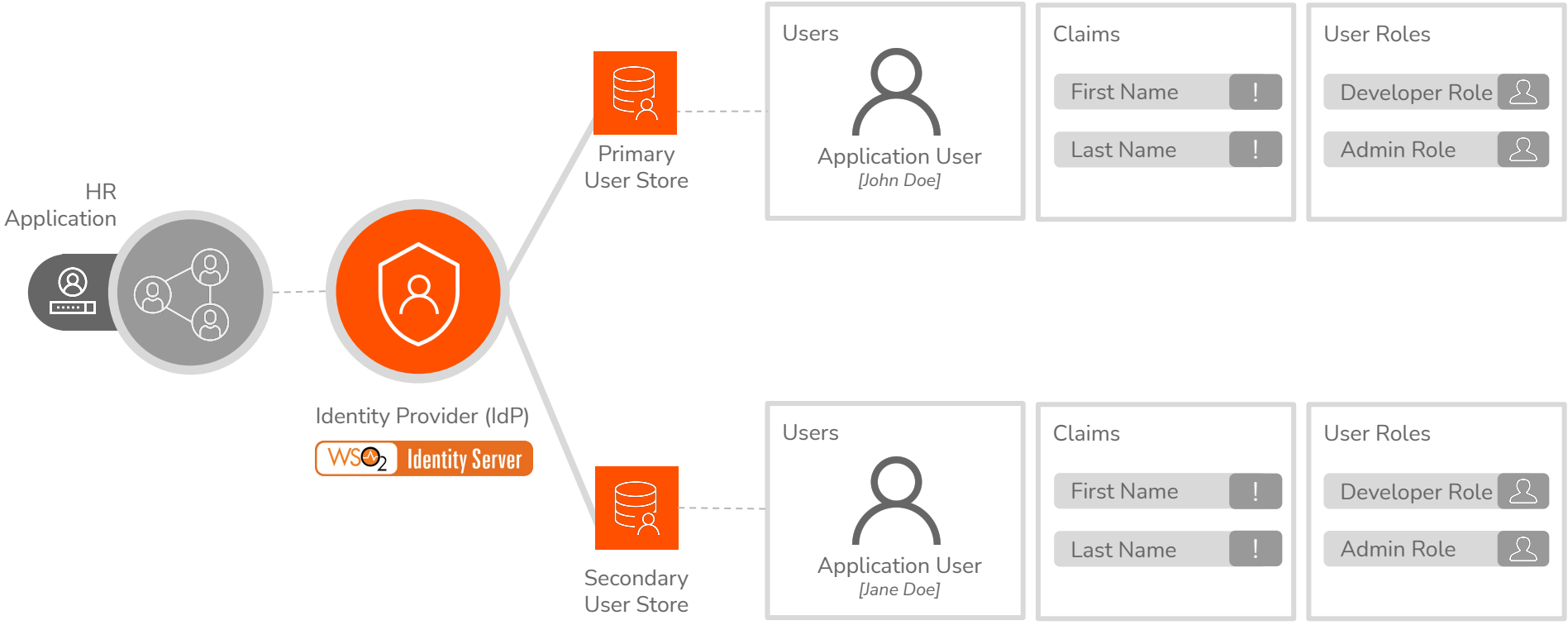
# Role-Based Access Control (RBAC)

- Resources are only accessible by the users assigned with particular user roles
- Reduced administrative costs
    - Ability to efficiently grant/revoke access to/from users by assigning/unassigning user roles
    - Ability to reduce/increase permissions for multiple users at once by simply modifying the related user role
- Easy to comply with regulations related to privacy

# User Stores

# User Stores

A repository that stores information on users and user roles



# Quick Recap

# What you learnt

1. Overview of users, claims, permissions, user roles, and user store
2. Role based access control

# Any Questions ?

Reach us through the following channels

iam-dev@wso2.org

https://stackoverflow.com/questions/tagged/wso2

https://wso2is.slack.com/

# Thank You