WSO2 IDENTITY SERVER

Introduction to Identity and Access Management (IAM)

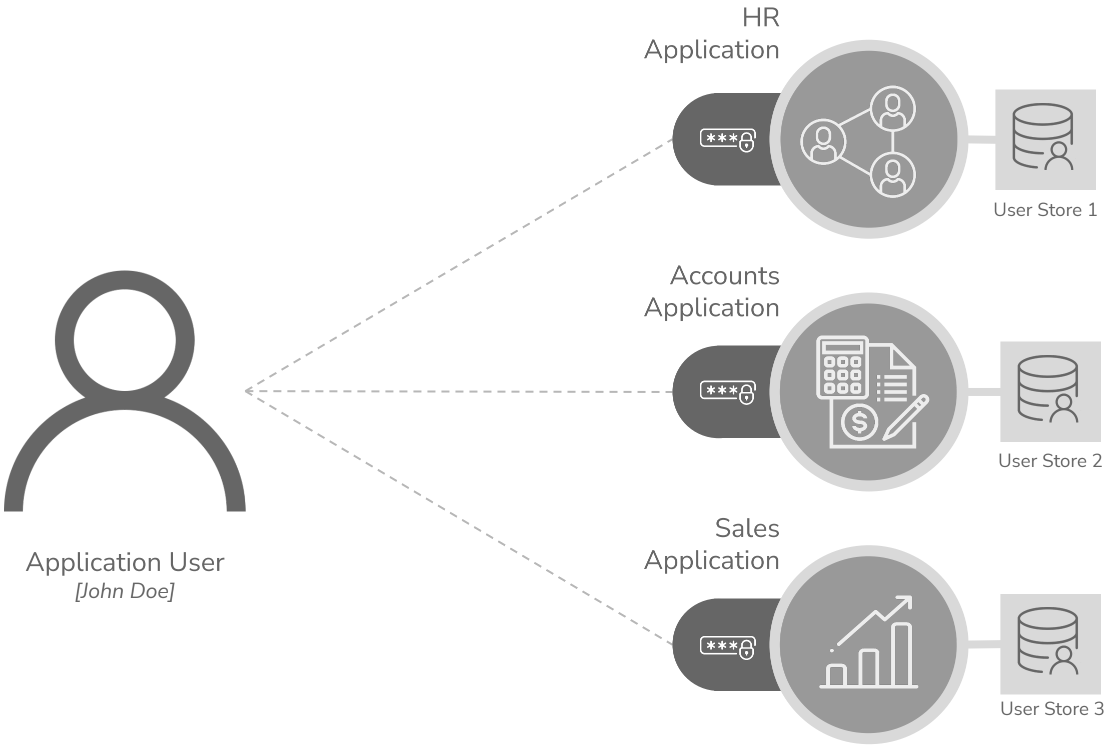
Why Identity and Access Management (IAM)?

- To securely store and manage user identities and access privileges
- To ensure that users are who they claim to be and grant access only if they have the permission to access
- To provide a better user experience (UX)
- To enable regulatory and privacy compliances
- To increases productivity and reduce IT costs

Traditional Access Management

Application-Level Access Management

Handling user authentication and account management at each application (traditional web app login)



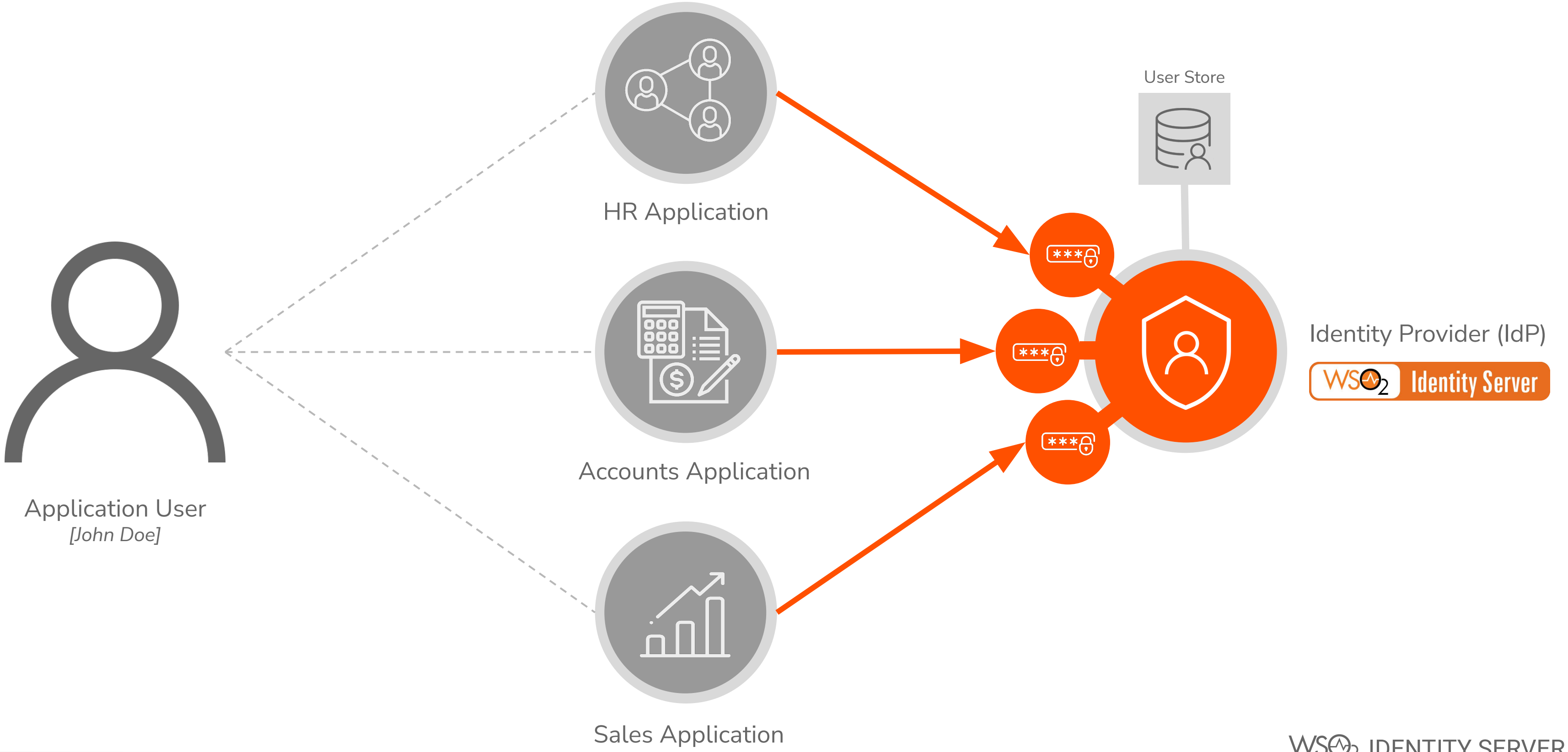
Issues with Traditional Access Management

- Higher chances of data breaching
  - Using simple passwords or same password for multiple applications
  - Security and account management is not a cornerstone in applications
- Minimum UX
  - Multiple login credentials to be remembered
  - Different login experiences in each application
- Difficulty in governance
- Less agility and low productivity
- High IT cost
- Difficulty in complying to regulations

Identity and Access Management Concepts

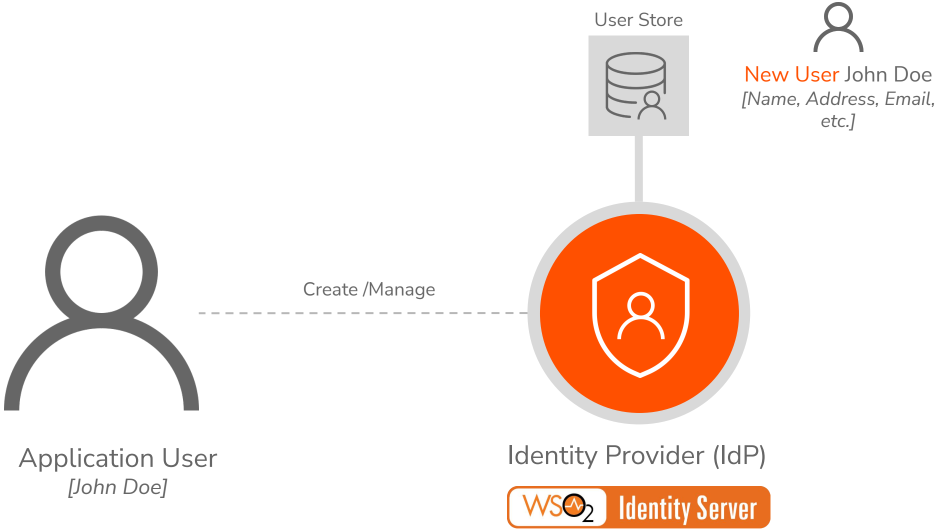
Centralized Access Management

Handling user authentication and account management at a central system



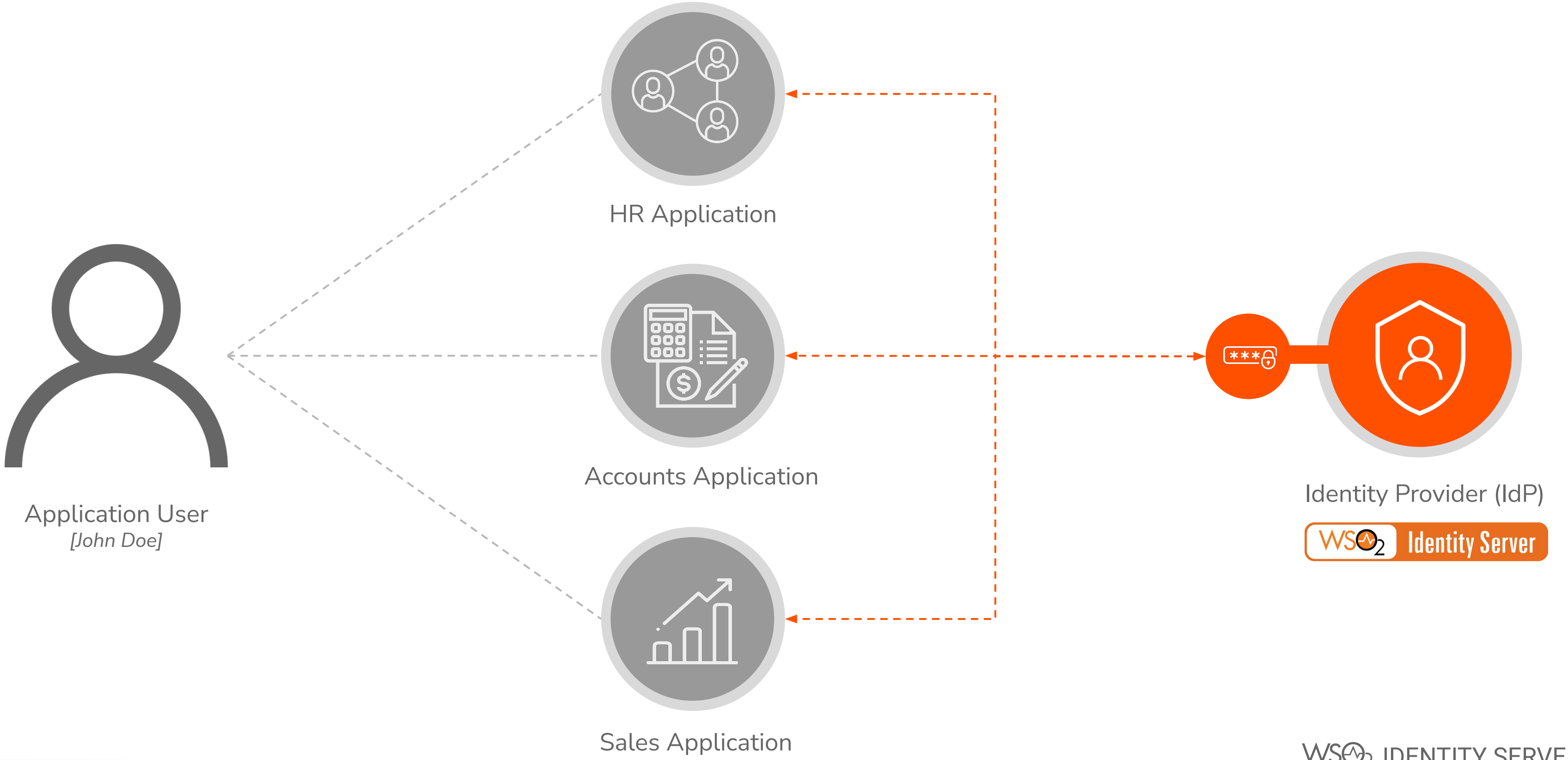
User Provisioning

Creating and managing user accounts/identity information within the system



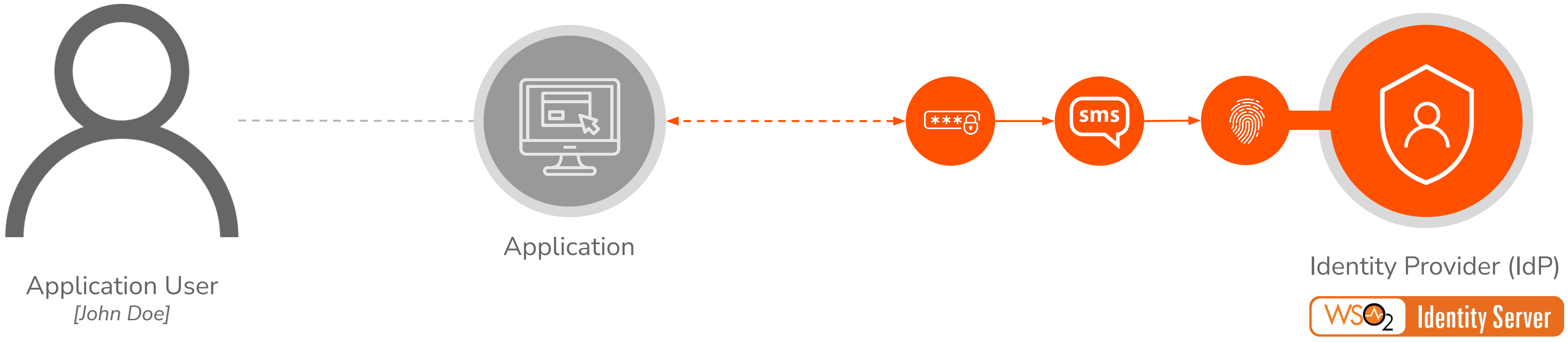
Single Sign-On (SSO)

Authenticating users once and allowing access to other associated applications



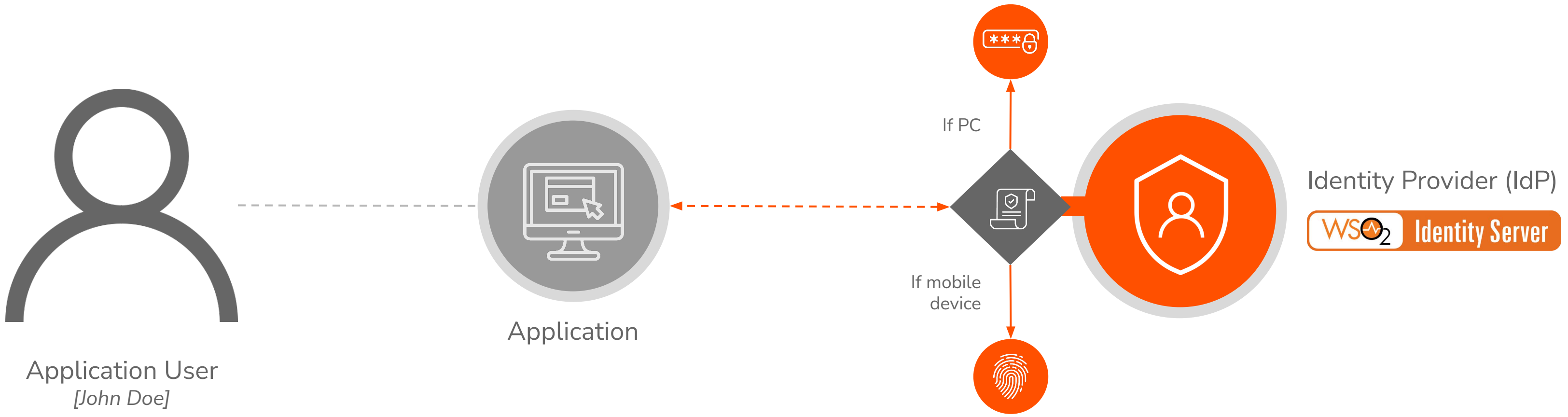
Multi-Factor Authentication (MFA)

Authenticating users by challenging with multiple authentication factors, e.g., password, SMS, and fingerprint



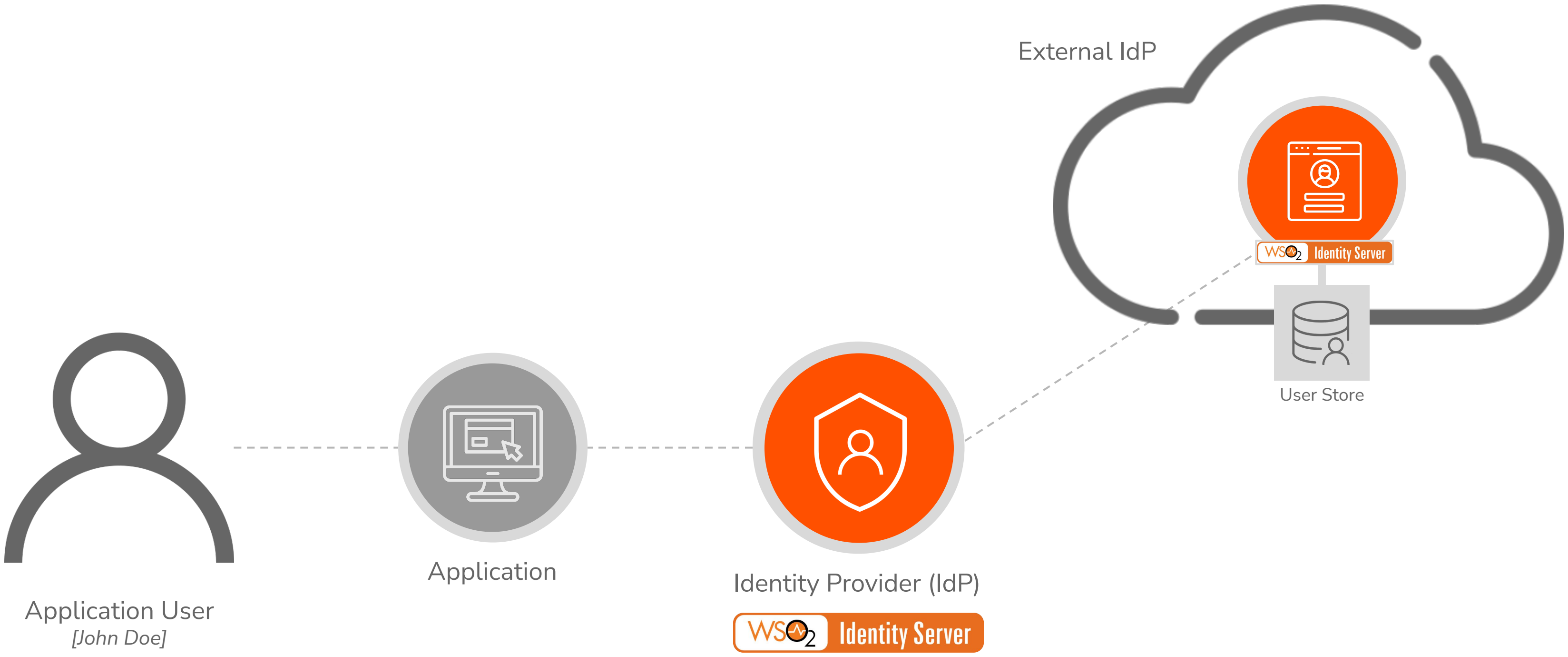
Adaptive Authentication

Authenticating users by challenging with multiple authentication steps based on the users’ risk profile



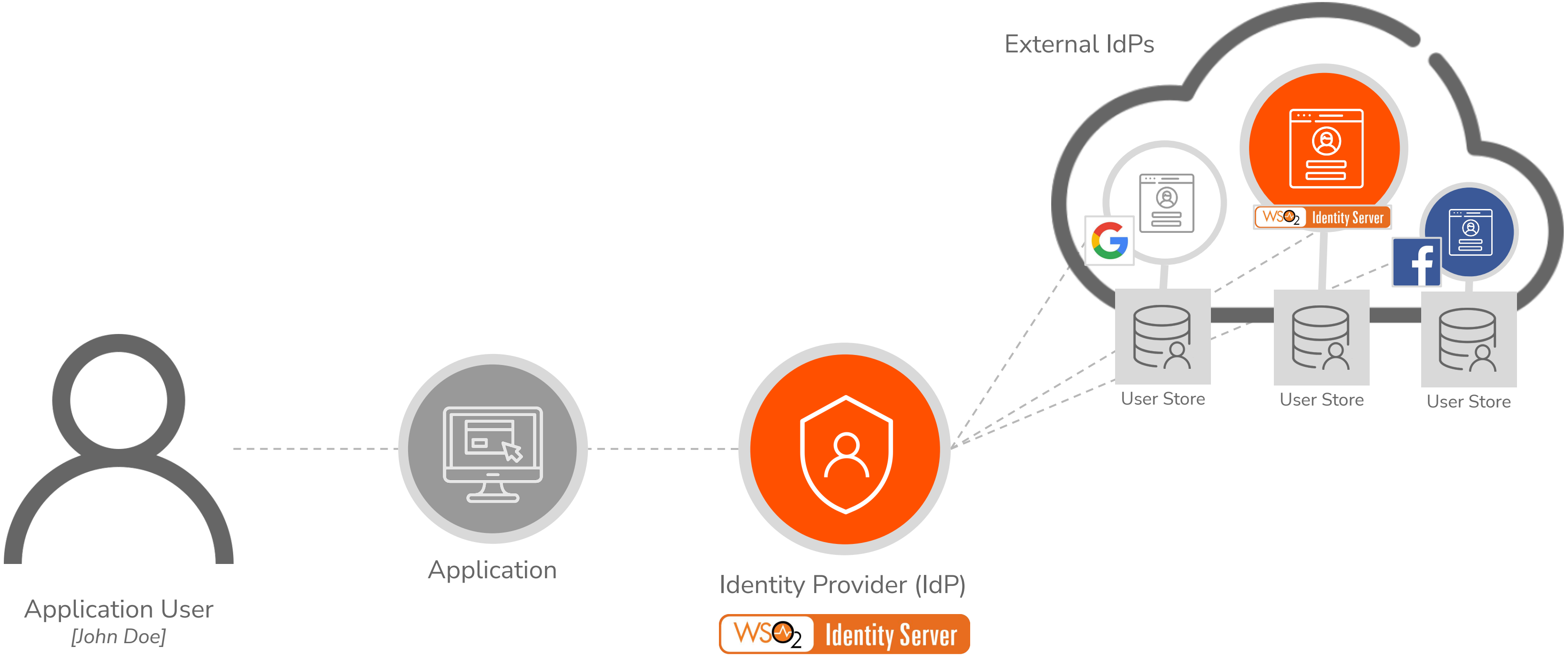
Identity Federation

Authenticating users existing in an external identity provider



Identity Federation with Social Login

Authenticating users using a social service provider as an external IdP



Privacy and Regulatory Compliance

GDPR
HIPAA
CALIFORNIA CONSUMER PRIVACY ACT
PSD2

Identity Provider (IdP)

WSO2 Identity Server

WSO2 Identity Server

Value Proposition

- Fully open source (Apache 2.0 open source license)
- Inherent extensibility for building tailor-made IAM platform
- 250+m identities managed worldwide
- 200+ production customers globally and 500+ educational institutes
- 24*7 support for the production customers
- Globally operating - main offices in USA, UK, Germany, Brazil, Australia, and Sri Lanka

Industry Recognition

kuppingercole ANALYSTS

Leader overall - KuppingerCole Leadership Compass on CIAM platforms - 2020

Strong performer - The Forrester Wave™ on Customer Identity and Access Management - Q4 2020

Leader overall - KuppingerCole Leadership Compass on Identity APIs - 2019

Product leader in LC: Access Management and Federation - 2018

Gartner peerinsights™

Gartner Peer Insights - Rating 4.3 (out of 5)

Key Features

- Web Single Sign-On (SSO) and Identity Federation
- Identity Bridging
- Adaptive and Strong - Multi Factor Authentication (MFA)
- Accounts Management and Identity Provisioning
- Fine-grained Access Control
- API Security
- Identity Analytics
- Privacy

Key Benefits

- Avoids vendor lock-in with open source and open standards
- Extensible architecture allowing customization to support unique IAM use cases
- Accommodates large-scale deployments with millions of users
- Effortless integration with cloud and on-premises applications, third-party authentication systems, and social identity providers
- Hassle-free deployment and low-cost maintenance

Quick Recap

What you learnt

1. Traditional access management and its issues
2. An overview to IAM concepts and benefits
3. WSO2 Identity Server features and benefits

Any Questions ?

Reach us through the following channels

✉ iam-dev@wso2.org

https://stackoverflow.com/questions/tagged/wso2is

https://wso2is.slack.com/

Thank You