WSO2CON 2024

Navigating IAM in the Modern Enterprise



Johann Nallathamby
Director - Solutions Architecture
WSO2



Malithi Edirisinghe
Director in Engineering
WSO2

Evolution of IAM in the Modern Enterprise

Evolution of IAM Business Requirements

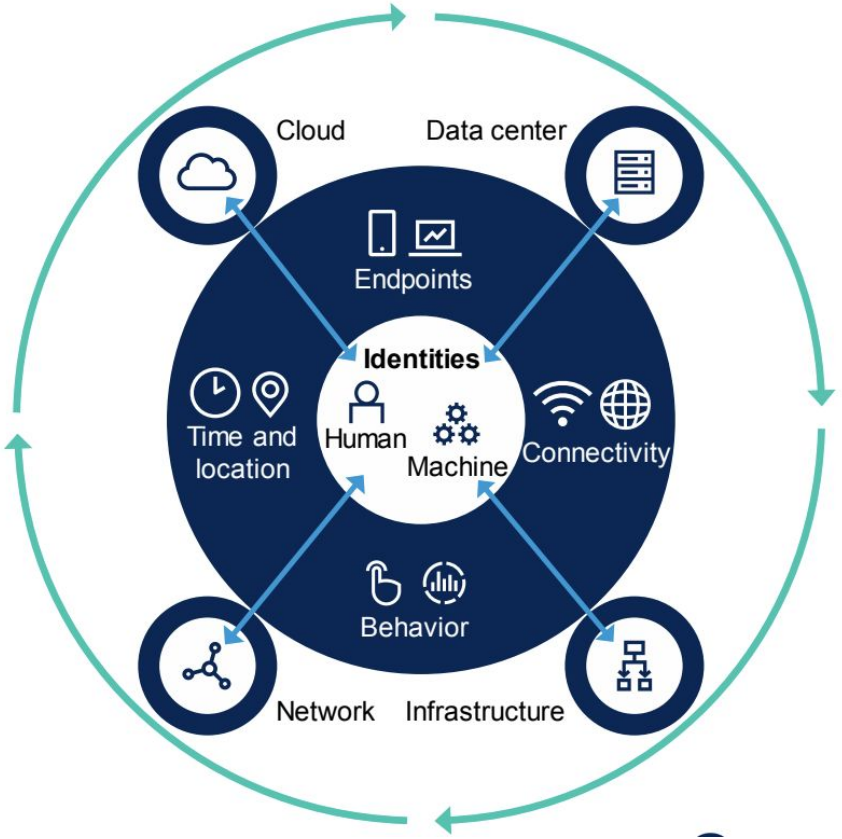
AREA	TRADITIONAL	MODERN	FUTURE
Scope	Organization only	Multiple organizations and public	Any human or machine
Topology	Siloed	Centralized	Centralized / decentralized
Architecture	Closed	Extensible and interoperable	Composable and orchestrated
Security	Physical perimeter	Logical perimeter	Adaptive, continuous, risk-aware and resilient
Standards	Few	Some	Pervasive
Connectivity	Siloed	Basic integration	Event-based
Change	Periodic	Frequent	Continuous and automated
Threat Detection and Response	None	Descriptive	Prescriptive and remediating
Privacy	None	Customers in selected regions	For everyone
Observability	None	Discovery within silos	Continuous

Identity-First Security

Consistent

Context-aware

Continuous



* Identity Fabric - The Definition and its Architecture - Felix Gaehtgens, Gartner IAM Summit 2024, London

Identity-first security is an approach that makes identity-based controls the foundational element of an organization's cybersecurity architecture

- Gartner -

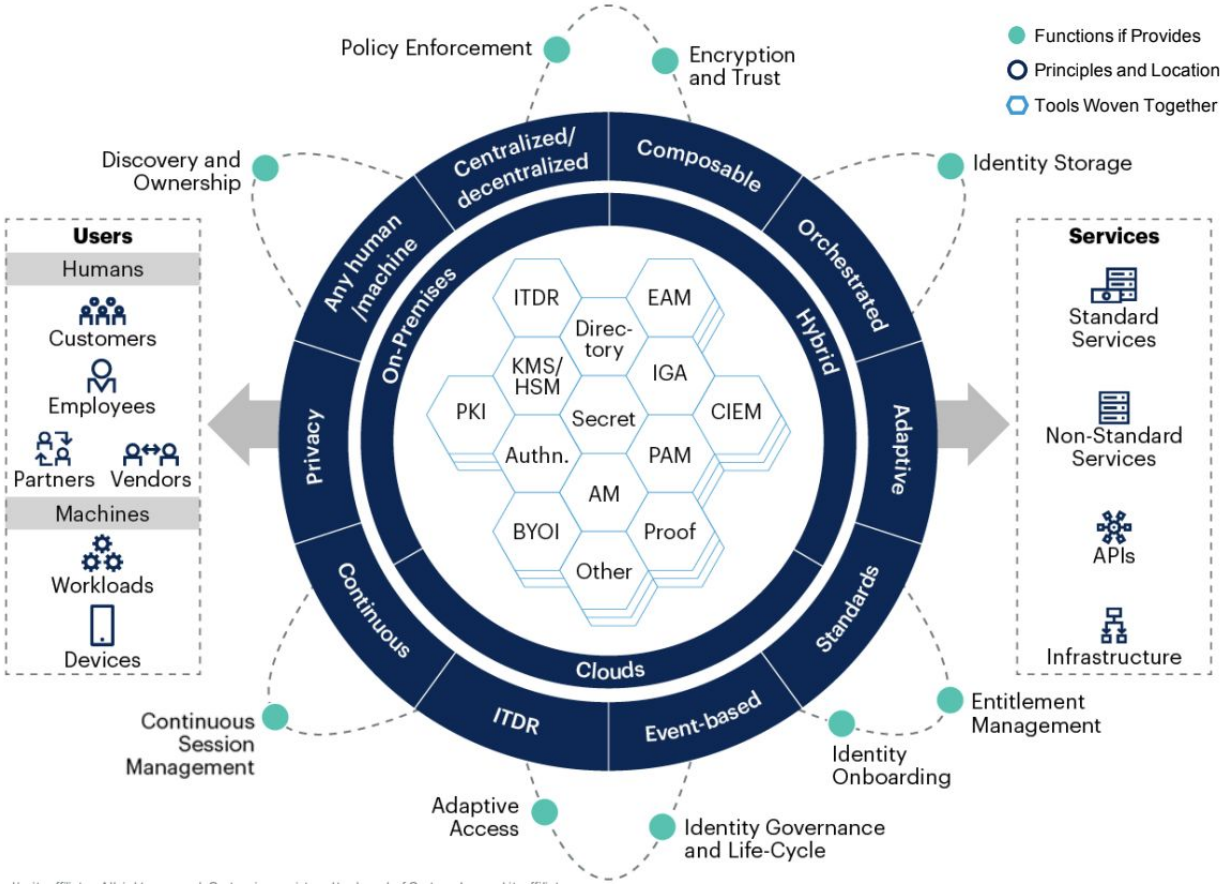


An identity fabric is an evolution of an organization's IAM infrastructure that is architected to enable identity-first security.

– Gartner –



Identitv Fabric



* Identity Fabric - The Definition and its Architecture - Felix Gaehtgens, Gartner IAM Summit 2024, London

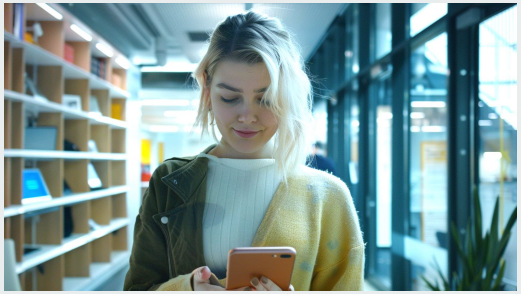
Open Standards – A must have for an Identity Fabric

STATUS	FOR ORGANIZATIONS AND APP DEVELOPERS	FOR IAM TOOL VENDORS
Existing	JWT, OAuth 2.0, OIDC, SCIM 2.0	FIDO2/WebAuthn, Radius, SAML
Early adoption	OPA, DID	SPIFFE, DID, Verifiable credentials
Emerging	SSE CAEP	
Nascent	SSE RISC, OIDC AuthZen	IDQL, WIMSE
Missing	SCIM for workloads and secrets	Better sharing of risk metadata

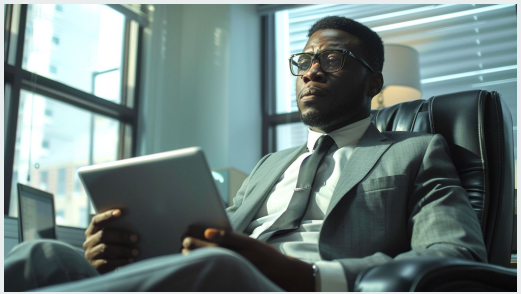
All Users Deserve Seamless and Secure Digital Experiences

Identity and Access Management

is fundamental to ensuring a long lasting, fruitful relationships with consumers, business partners and employees.







IAM Landscape

IGA | **PAM** | **WAM**

Access Management

B2C



- Self-registration and social-login
- Identity verification
- Account linking
- Progressive profiling
- Passwordless, OTP and Adaptive MFA
- Consent-based authorization
- Branding and internationalization
- Login and registration insights

B2B



- Distinct tenancies per organization
- Flexible organizational hierarchy design
- Enterprise login
- Customizable login experiences for organizations
- Delegated administration
- B2B Collaboration

B2E



- User invites and bulk onboarding
- BYO-directory/Virtual directory
- Just-in-time access provisioning
- Single sign-on
- X509, RSA, IWA and Adaptive MFA
- Role-based authorization

APIs



- OAuth 2.0/OIDC compliance
- Consent-, role- and context-based authorization
- Pre-integrated API gateways

3 Key Stakeholders that an IAM solution MUST Satisfy



Empower developers



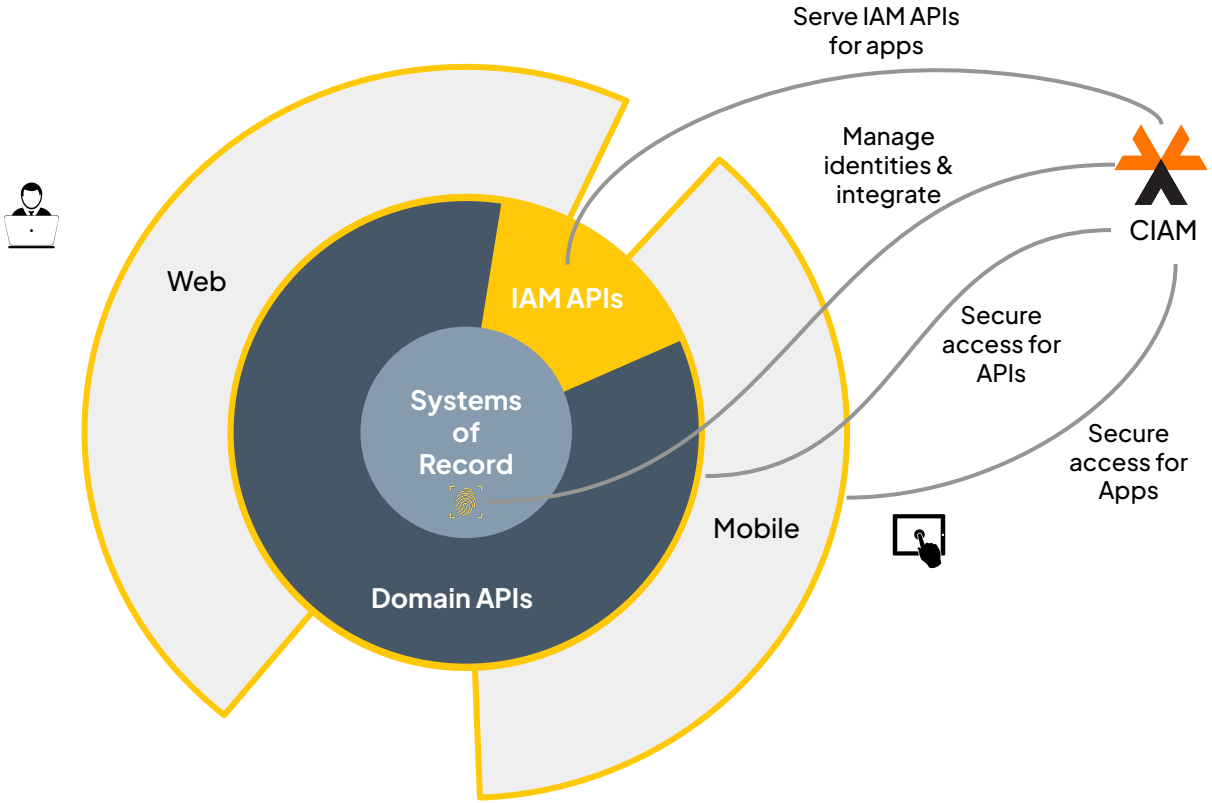
Enhance customer experiences



Optimize internal processes

CIAM for consumer facing applications

What CIAM means for your consumer facing applications ?



The significance of CIAM in consumer applications

Adoption

Frictionless registration and login is the entrypoint for your apps

and the key for adoption.

An identity-centric approach is crucial for delivering exceptional digital experiences.

Security

Consumer data must be safeguarded at every step.

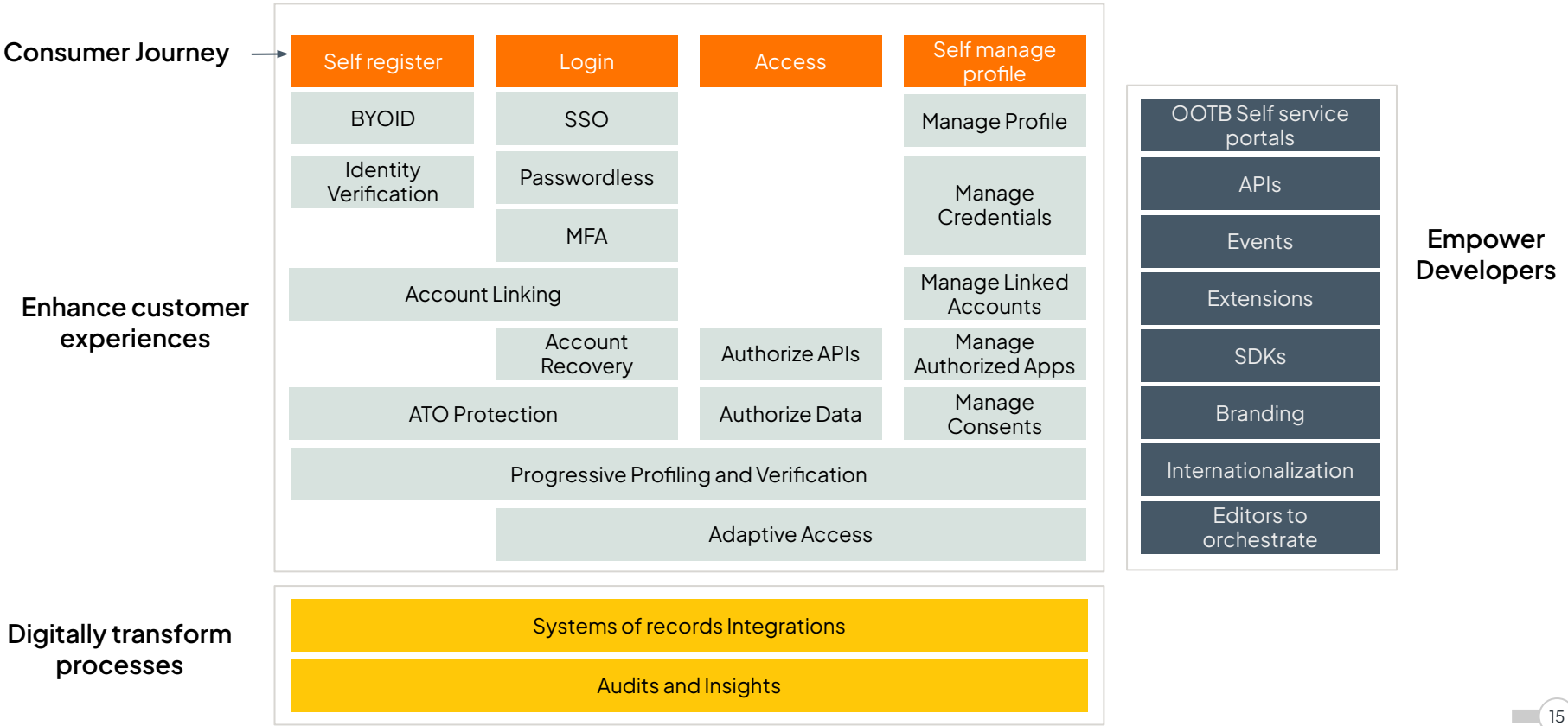
Identity verification, authentication, access authorization, and continuous access evaluation are the essential building blocks.

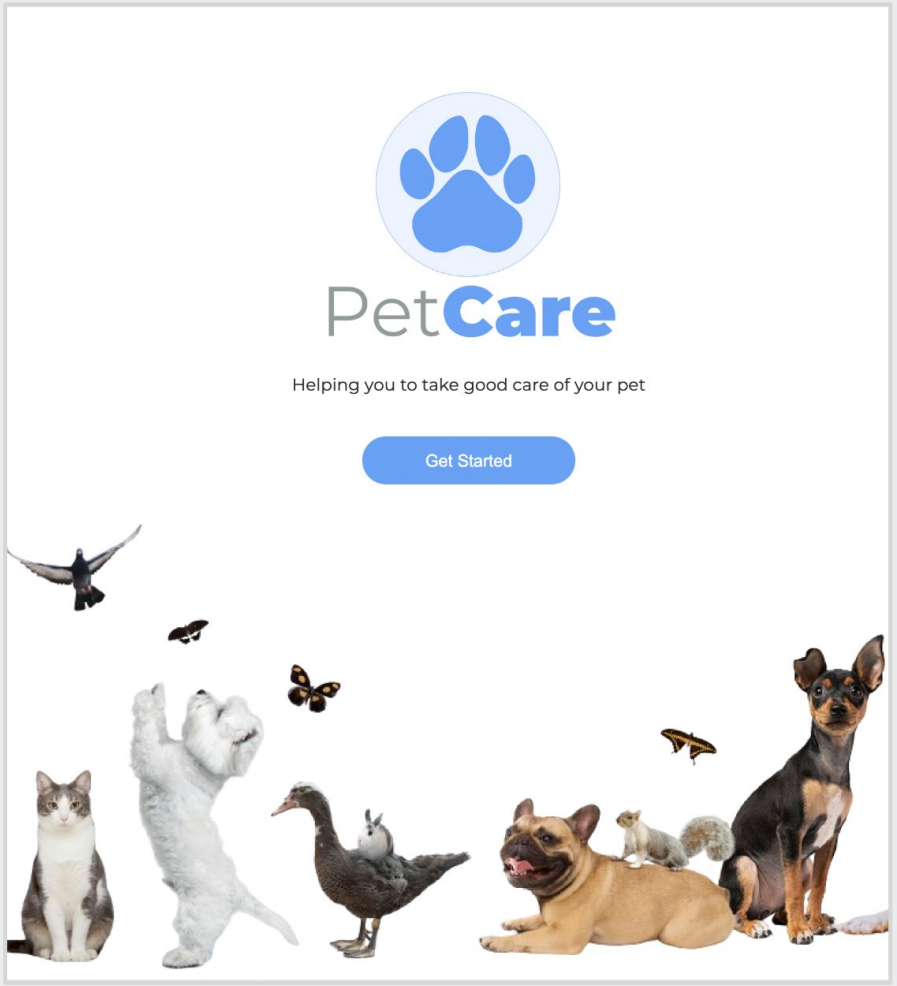
Compliance

Compliance with data protection regulations is essential.

CIAM solutions are designed with compliance in mind, ensuring adherence to standards like GDPR, CCPA, PSD-2, and more.

Critical Requirements for effective CIAM in consumer apps





Let’s start managing access for a web application

Best practices for web apps implementing OAuth/OIDC

Single Page Apps (SPAs)

Rely on JavaScript and render the content in the browser without page refresh.

- Use Authorization Code Flow with PKCE
- Secure API Requests
- Use short lived tokens
- Use BFF pattern when possible

  Choreo managed authentication

  Not opting for BFF ? Carefully choose the token storage

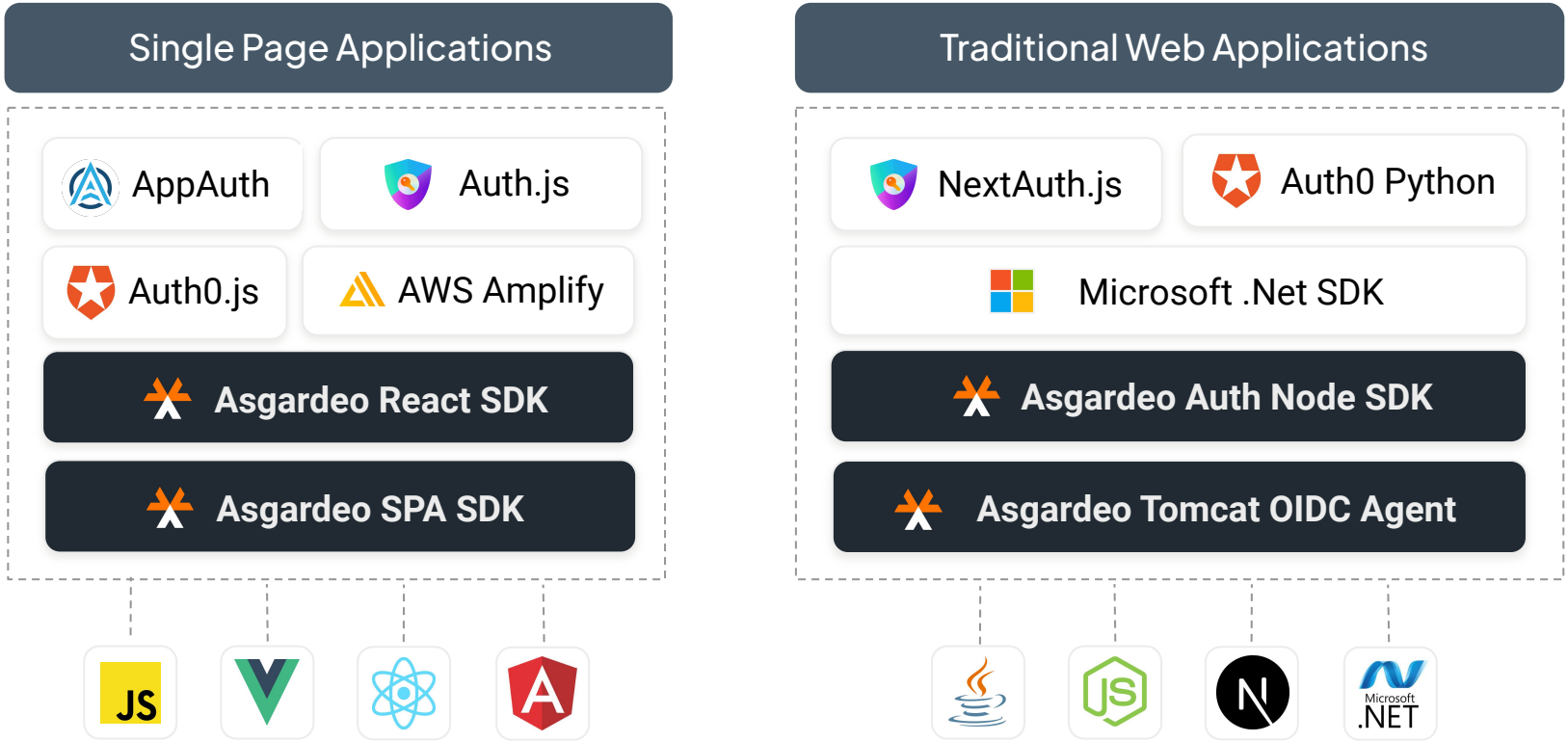
  webworker or session storage or local storage

Traditional Applications (MPAs)

Loads a new page from the server as user interacts resulting a page refresh.

- Use Authorization Code Flow with PKCE is still recommended
- Secure API requests
- Implement proper session management
- Regularly rotate secrets

Use well known libraries



Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce

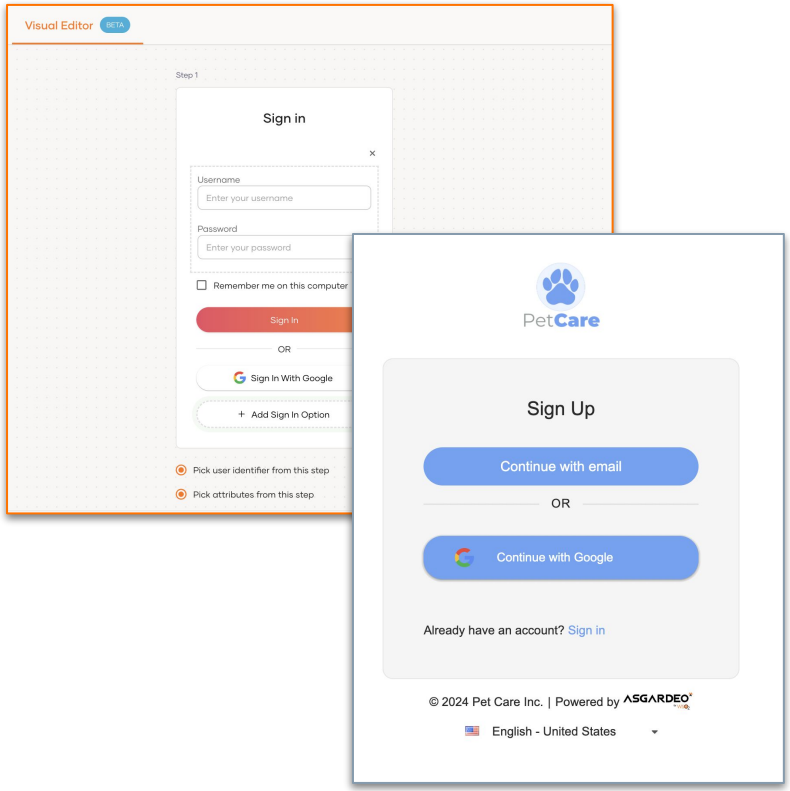


Clone the iam-tutorial repo to follow



Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce

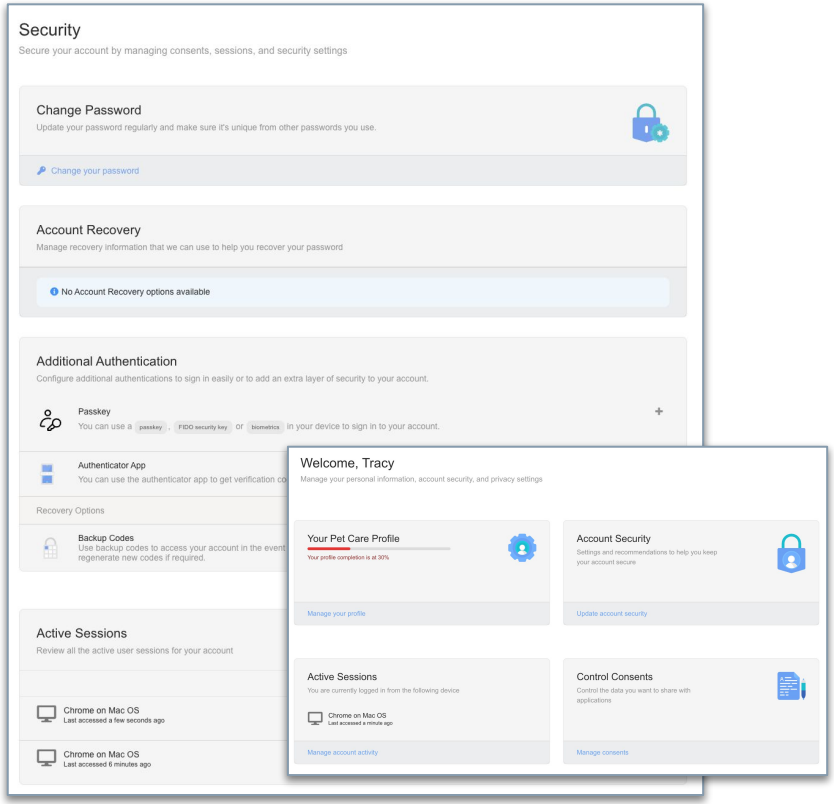


Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce

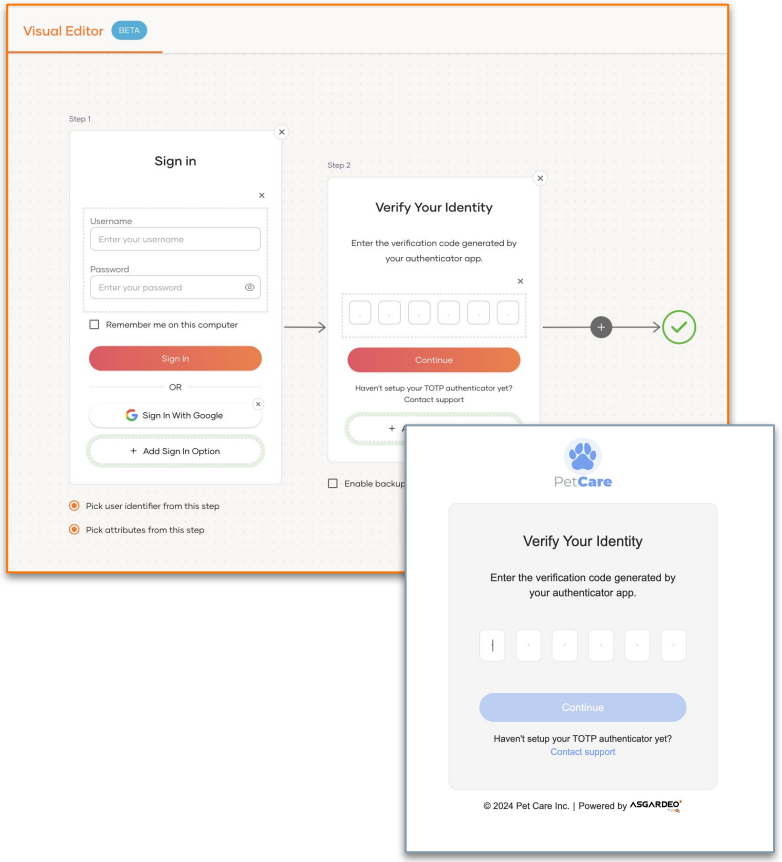
Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce



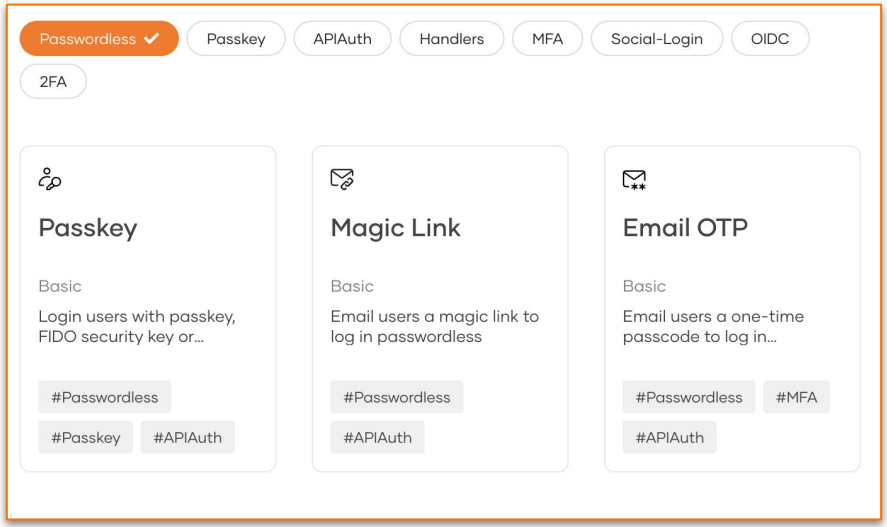
Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce



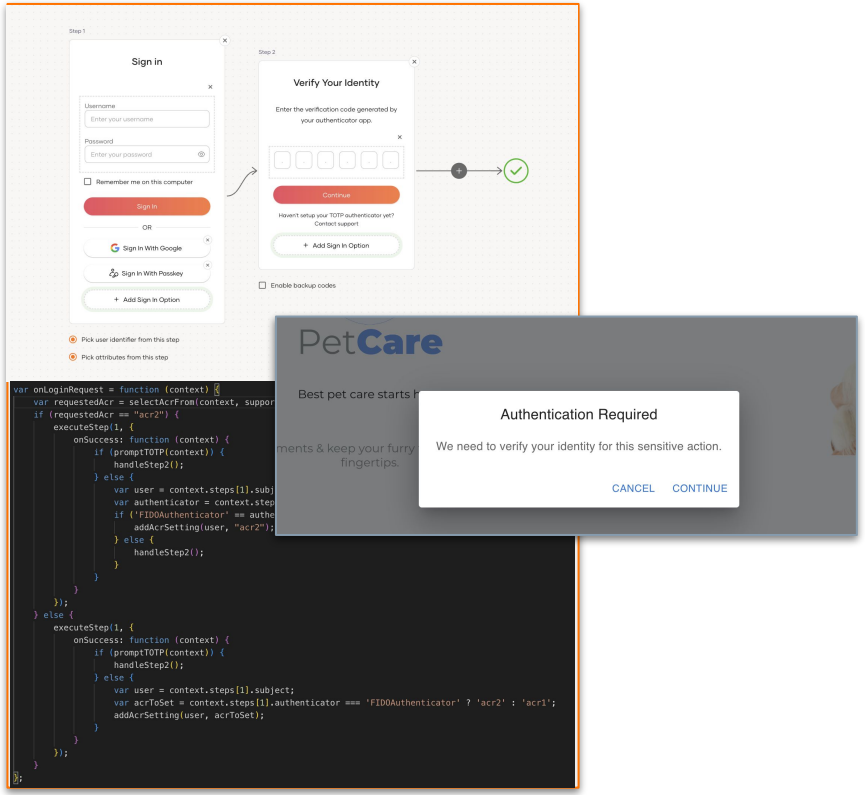
Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Single Logout (SLO)
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce



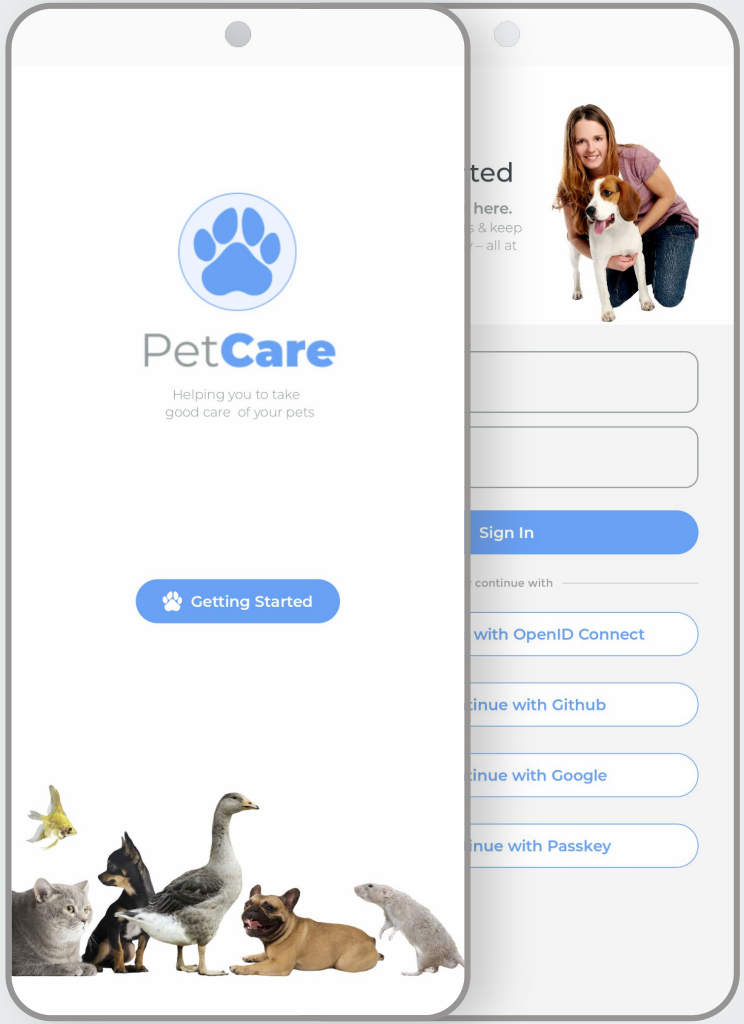
Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Single Logout (SLO)
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce



Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Single Logout (SLO)
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce



Implement omni-channel experience with mobile

Best practices for mobile apps implementing OAuth/OIDC

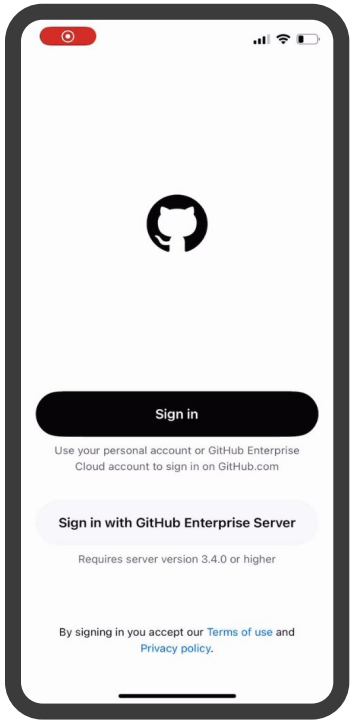
- Use Authorization Code Flow with PKCE
- Use In-app browser tabs that utilize system browser to redirect
- So much to handle ? Use libraries

   AppAuth.io
- Store tokens securely

  iOS -> KeyChain

  Android -> EncryptedSharedPreferences

Prefer the redirect based UX for Login ?



GitHub mobile app for iOS

Disconnected experience with redirection to the Authorization Server (AS)

User sees the domain and knows the site being redirected is legitimate still.

Introducing API for In-App Authentication

CURRENT USER EXPERIENCE

An external browser window is required to handle logging into the app



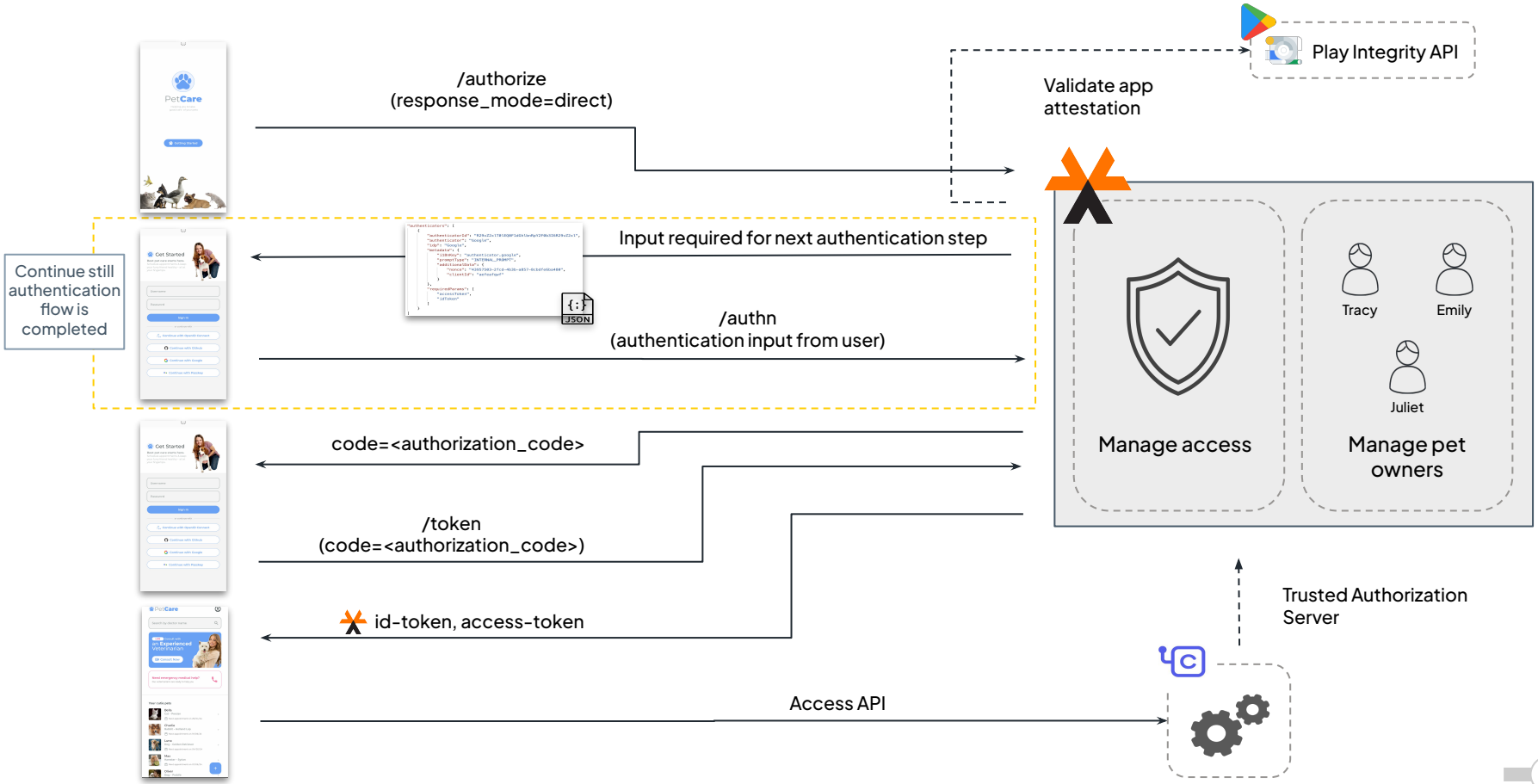
NEW USER EXPERIENCE

User never leaves the native application while logging in



- Use extended OAuth 2.0/Open ID Connect flows in an API centric way without redirecting to a browser Internet-Draft:draft-parecki-oauth-first-party-apps
- Orchestrate authentication conditionally without changing the application logic
- Guarantees the identity and proof of possession of the client and the API only communicates with legitimate client apps

In-App Authentication for Mobile App in Action



Using Asgardeo SDKs to simplify In-App Auth development

Developing Android Apps?

Use the Android SDK by Asgardeo

 Android SDK

iOS SDK Coming Soon!

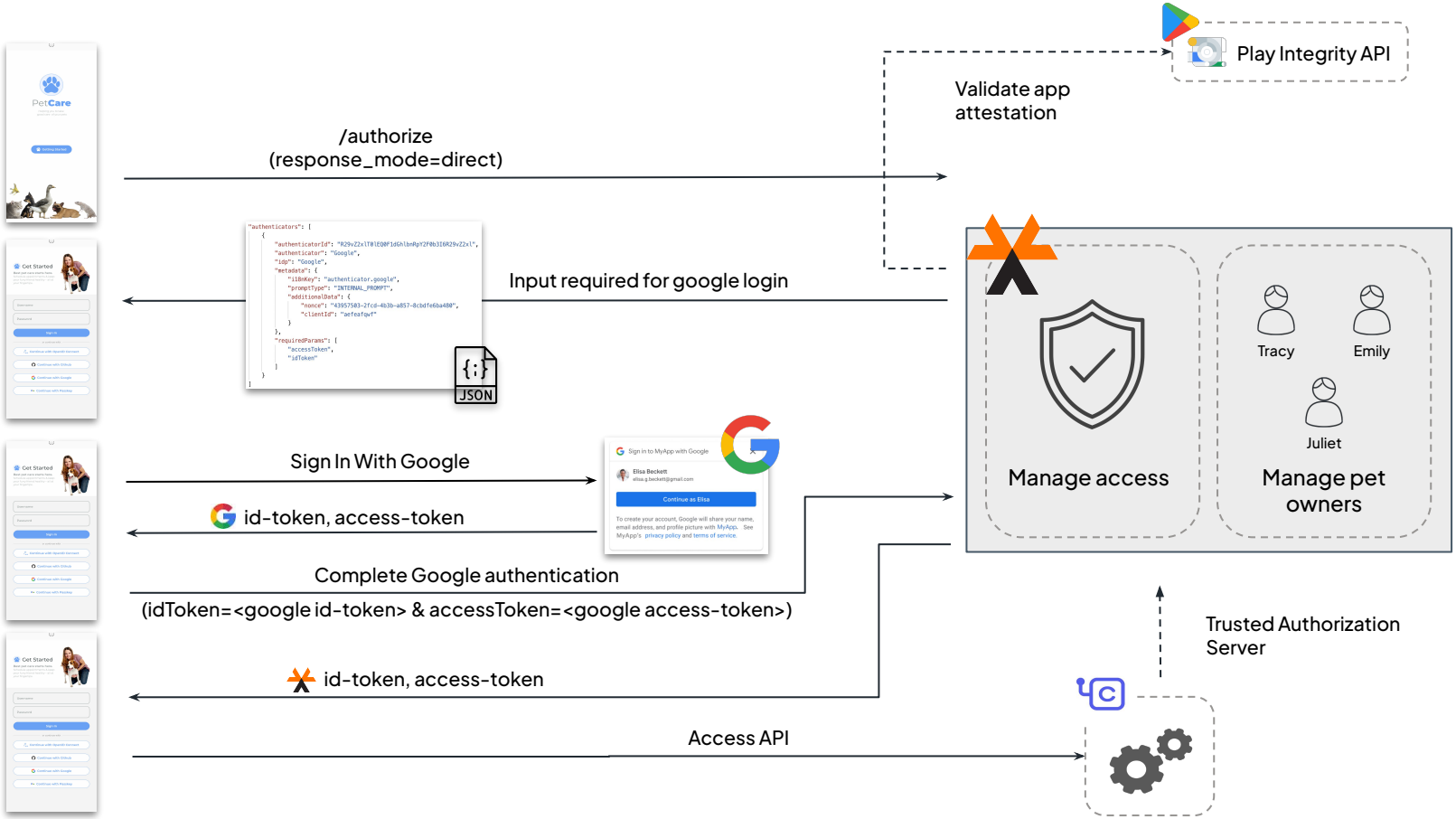
Federating to a third party Identity Provider

Supports integrating natively or over redirection.

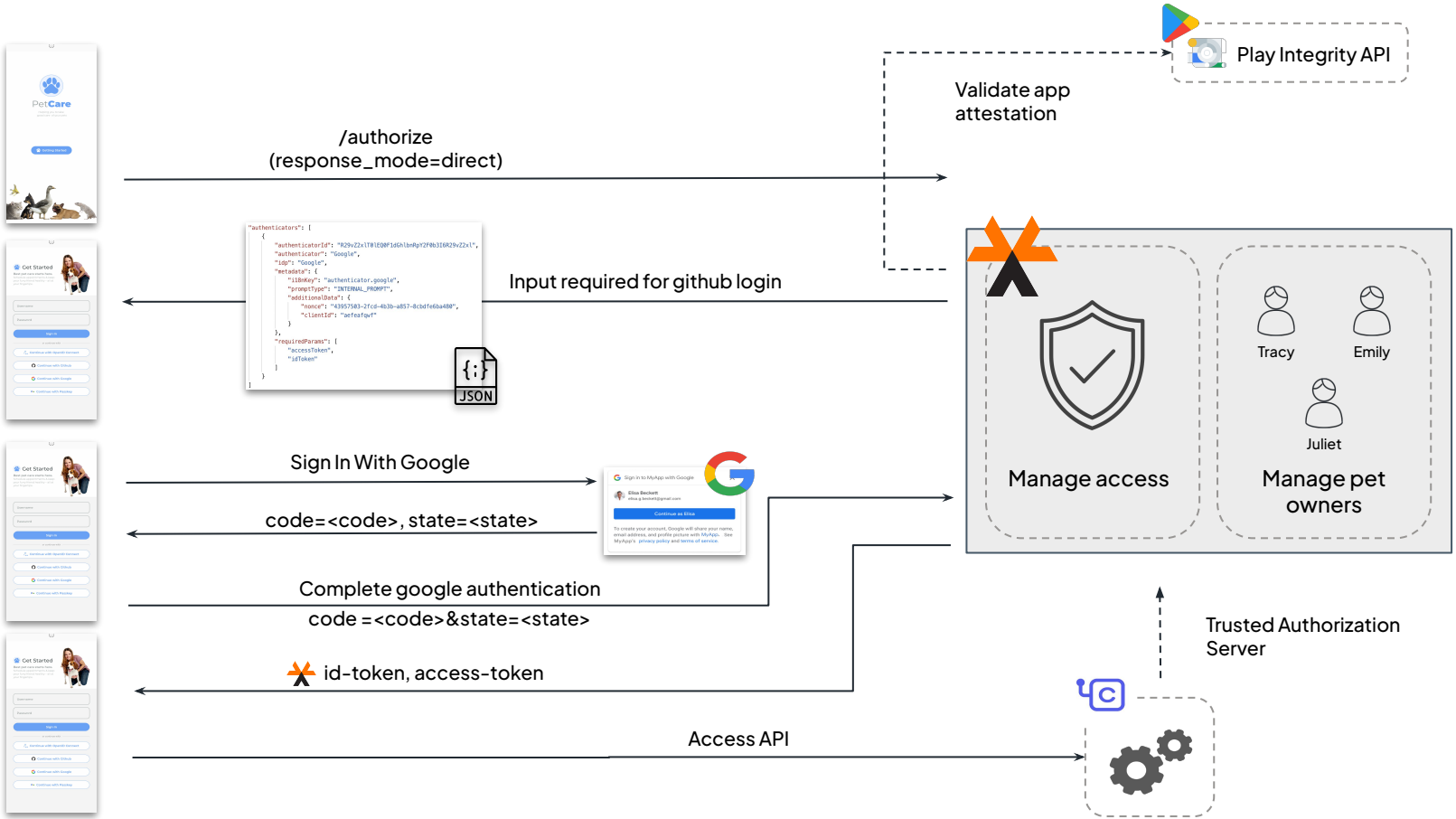
- Native
  - Use SDKs provided by Social Login Identity Providers for the platform

    e.g, Google, Apple
  - Create back the session in AS (Asgardeo/Identity Server) with id-token
- Redirect
  - Redirect to the authorization URL AS (Asgardeo/Identity Server) sends in the API flow
  - Use when platform native SDKs are not available or when redirection is ok

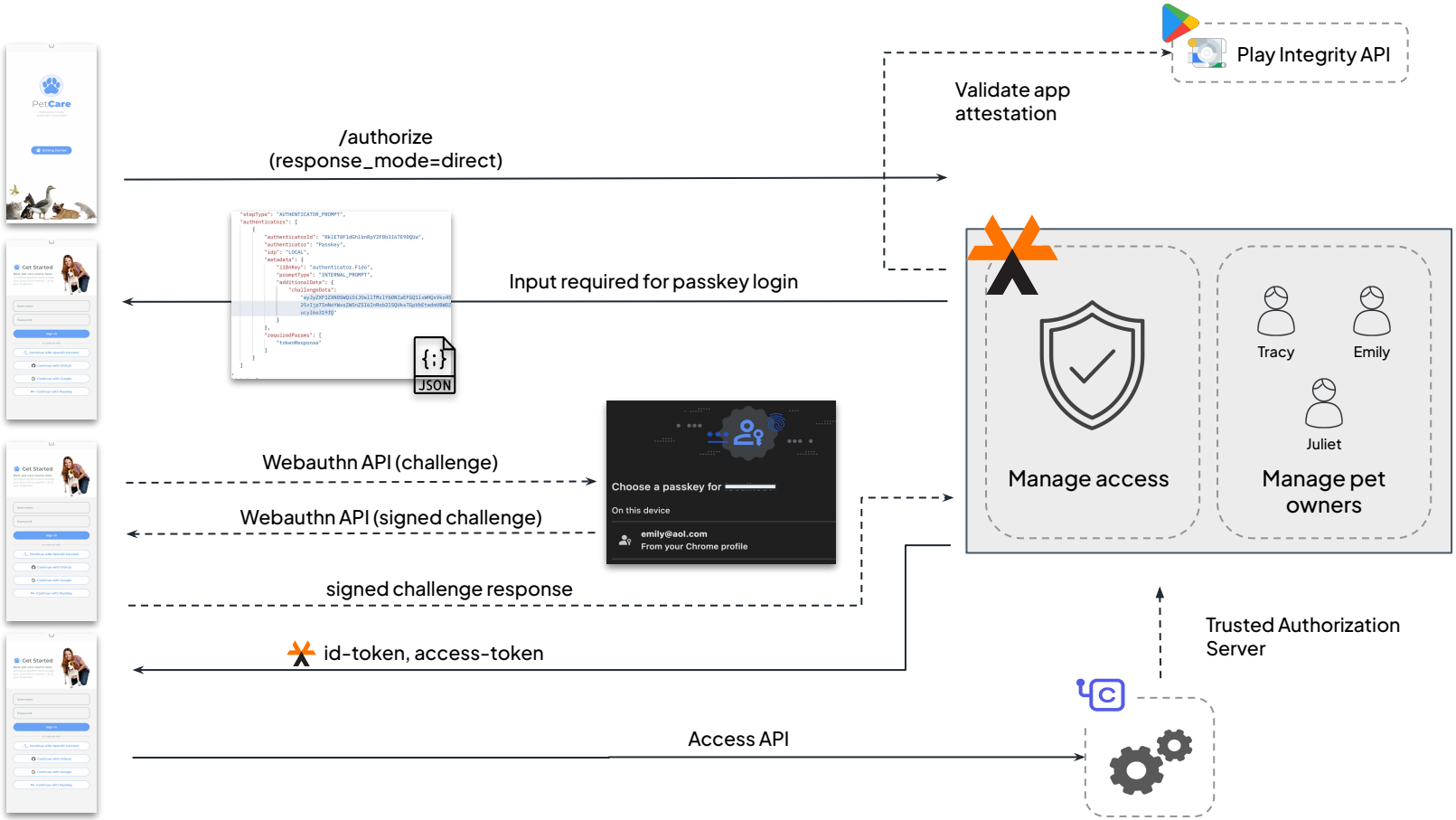
Add Login with Google natively



Add Login with Google redirecting to the browser

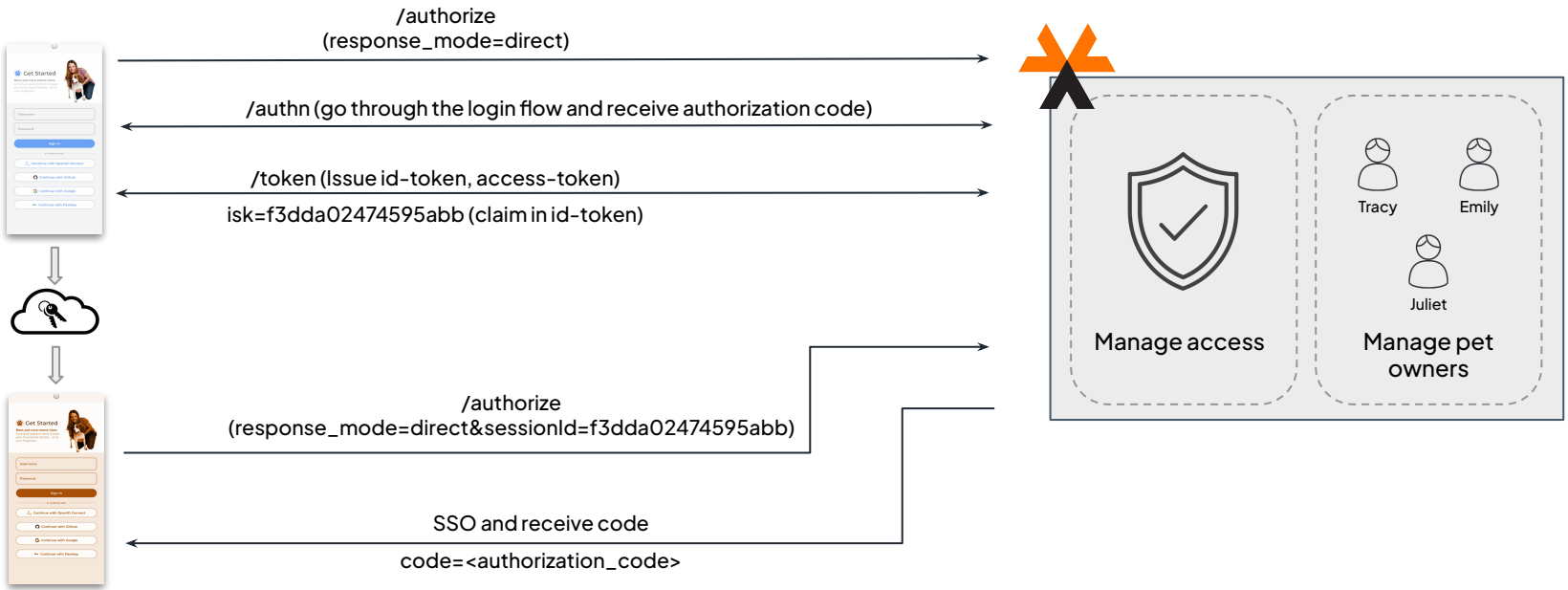


Add Login with Passkeys



SSO over In-App Authentication API for mobile apps

Initiate the authorization request with the session identifier accessible over the secure shared storage between apps



Intended only for native applications ?

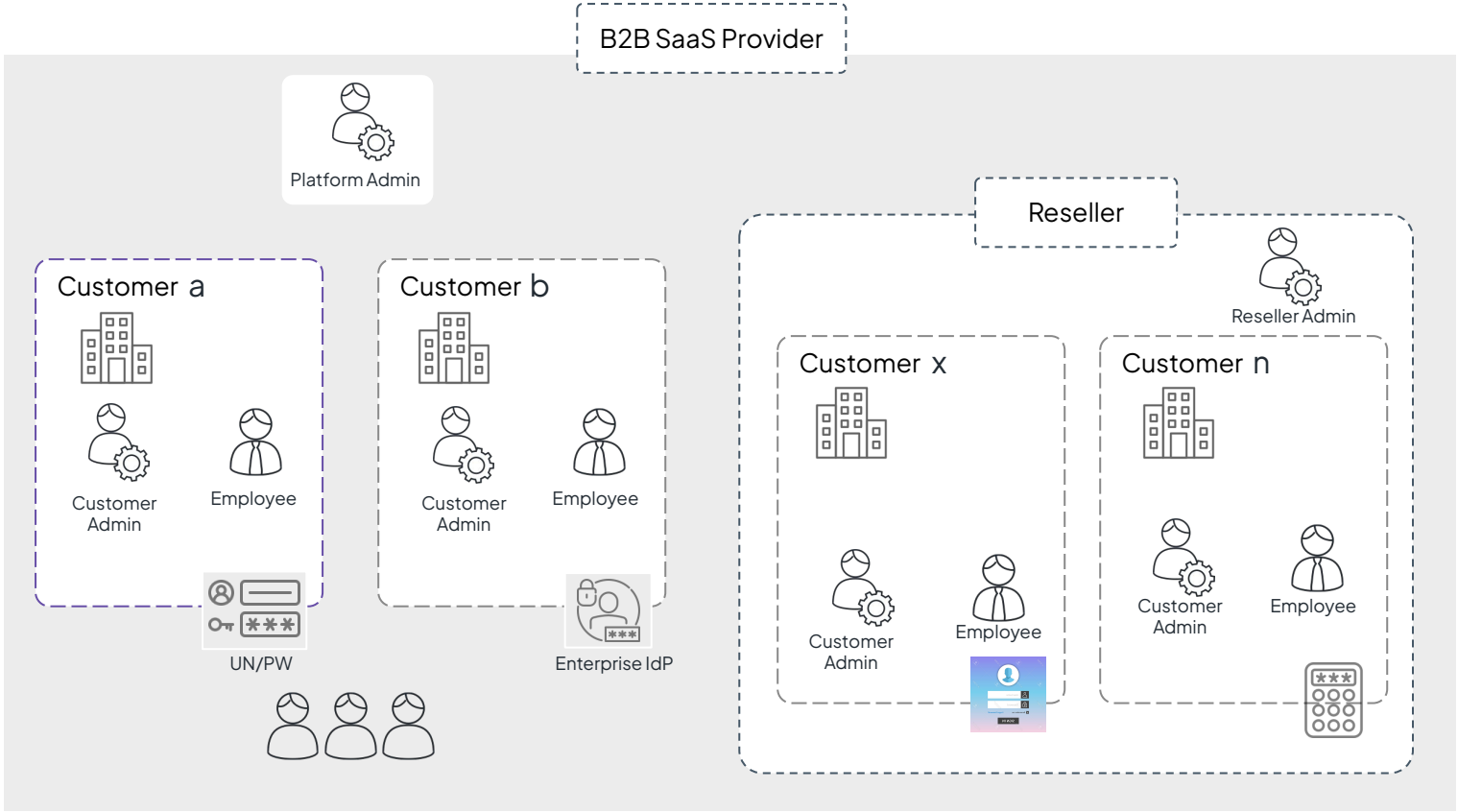
- Use wherever enhanced flexibility and control over user experiences during login and access are required, subject to the following:
  - Use only for first party apps
  - Use only with confidential clients with client authentication
    - Use client authentication mechanisms available for the confidential clients in the authorization endpoint when response_mode is “direct”
    - Ability to mandate the Pushed Authorization Requests (PAR) requests and use client authentication

Upcoming roadmap for In-App Authentication

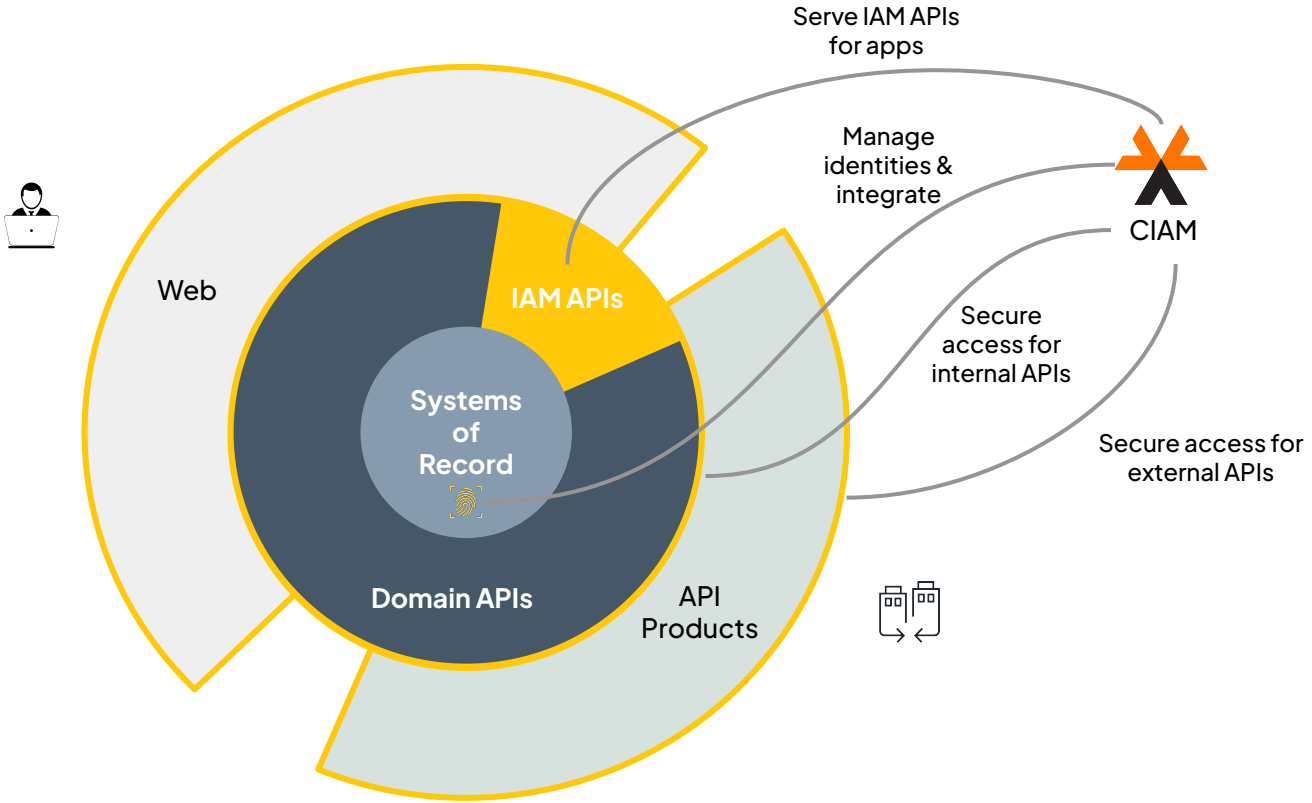
- SDKs for iOS and Flutter
- Improved support for redirect flows
  - Support to handle implications of using deep links in web clients of some of the social login providers. E.g: Google, Facebook
- Comprehensive support for diverse steps in the login flow

CIAM for B2B Interactions

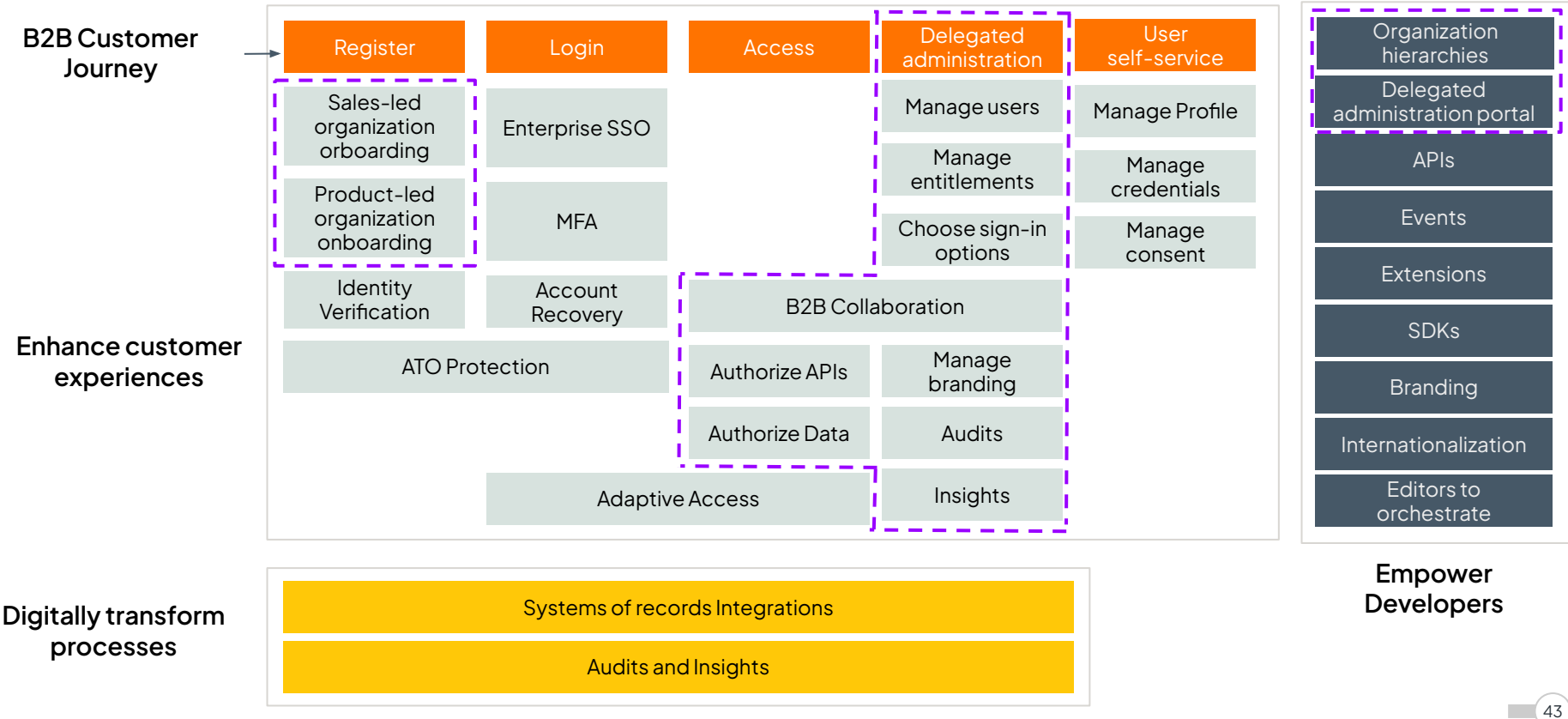
B2B Organization Management



What CIAM means for your B2B users?



Critical capabilities for effective CIAM in B2B SaaS apps



Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Managing access for B2B SaaS applications

- Authorizing APIs for B2B SaaS applications
- Managing organizations
- Delegating administration
- Custom login journeys per organization
- Custom branding per organization
- Selective application subscription
- Modeling organization hierarchies

Pathway for successful CIAM Strategy

- Focus on domain logic, use CIAM platforms

  Prioritize your core business processes while leveraging CIAM platforms to manage identity and access.

- Shift to Multi-Experience CIAM

  Design CIAM strategies that support multiple user experiences, offering a flexible and user-friendly approach.

- Conduct comprehensive stakeholder assessments

  Consider all external stakeholders to ensure that CIAM addresses user experience, business, technical, and regulatory requirements.

- Select flexible and extensible tools

  Opt for CIAM platforms with open integration standards and customizable workflows, ensuring adaptability and scalability.

A Single Product Powering Multiple Deployment Options to Support Any IT Strategy



WSO2 Identity Server

The Leading Open Source IAM

WSO2 Identity Server is a powerful, modern identity and access management solution for your on-premises or cloud environment

ASGARDEO

Multi-tenant SaaS IAM

Asgardeo is a developer-focused, multi-tenant IDaaS solution that provides seamless, secure authentication and user management

WSO2 Private Identity Cloud

Single-tenant SaaS IAM

Private Identity Cloud is a single-tenant cloud deployment of Identity Server, fully managed and maintained by WSO2

Advancements in IAM Preparing for Tomorrow

1. Future-Proofing IAM Against Post-Quantum Threats

Impact upon the arrival of Quantum Computers

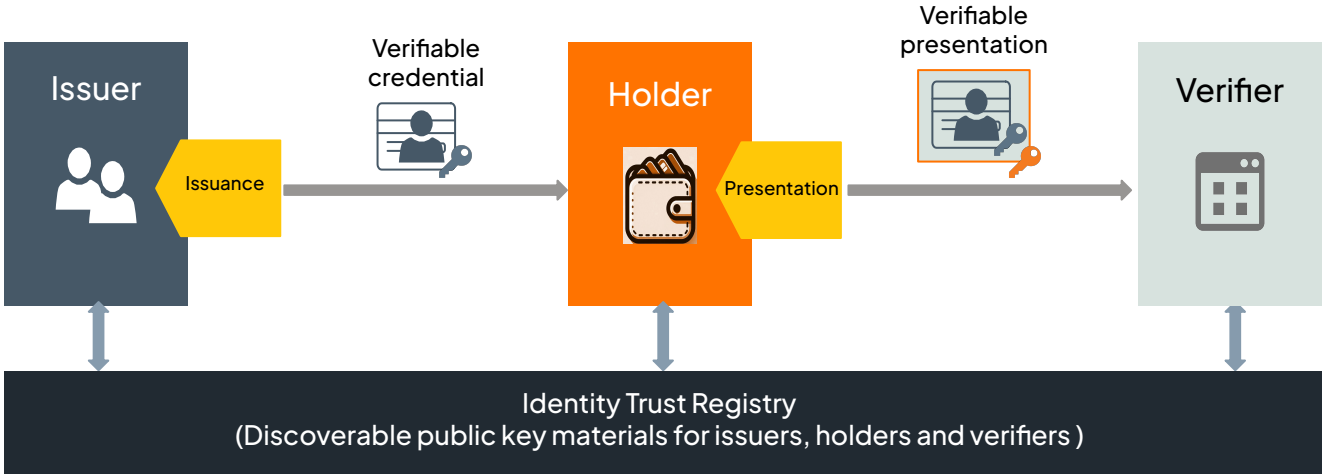
- Ability to break public-key cryptosystems* and less robust symmetric cryptosystems* currently in use
  - An attacker can store encrypted data today, and decrypt it when they gain access to a quantum computer (store-now-decrypt-later (SNDL) attack).
  - Possibility of reading persisted states over data transmitted via HTTPS or data encrypted at rest.
  - Less impact on signature validation scenarios due to short lived, temporal nature of data that transmits.
- Less robust hashing* techniques will be prone to brute force attacks
  - Possibility of credential bruteforce with hashing.

Act now before it's too late.

- Upgrade HTTPS communications to PQC enabled TLS.
- Use at least AES-128 in symmetric cryptosystems and SHA-256 in hashing use cases
- Make your systems crypto-agile so you can act fast.

* NIST Post Quantum Cryptography

2. Decentralized Identity and Verifiable Credentials



2. Decentralized Identity and Verifiable Credentials

Key value propositions to monitor

- Non auditing Identity Providers is a key advantage
- Facility for ubiquitous high assurance credentials and scalable verification

Current trend and joining the movement

- Current adoption is focused on Identity Wallets
  - EU Digital Identity wallet is closer, and wallet implementations are getting standardized
- Trust infrastructure decentralization remains challenging
- DCI ecosystems are forming around, so better join the ecosystem integrating issuers, verifiers and wallets as applicable

- Technical Insights: Decentralized Identity and Verifiable Credentials Trends and Advancements -Gartner IAM Summit 2024, London
- Verifiable Credentials for the Identity Practitioner - Identiverse 2023

3. The Interplay of AI in Digital Identity

Personalized Experiences

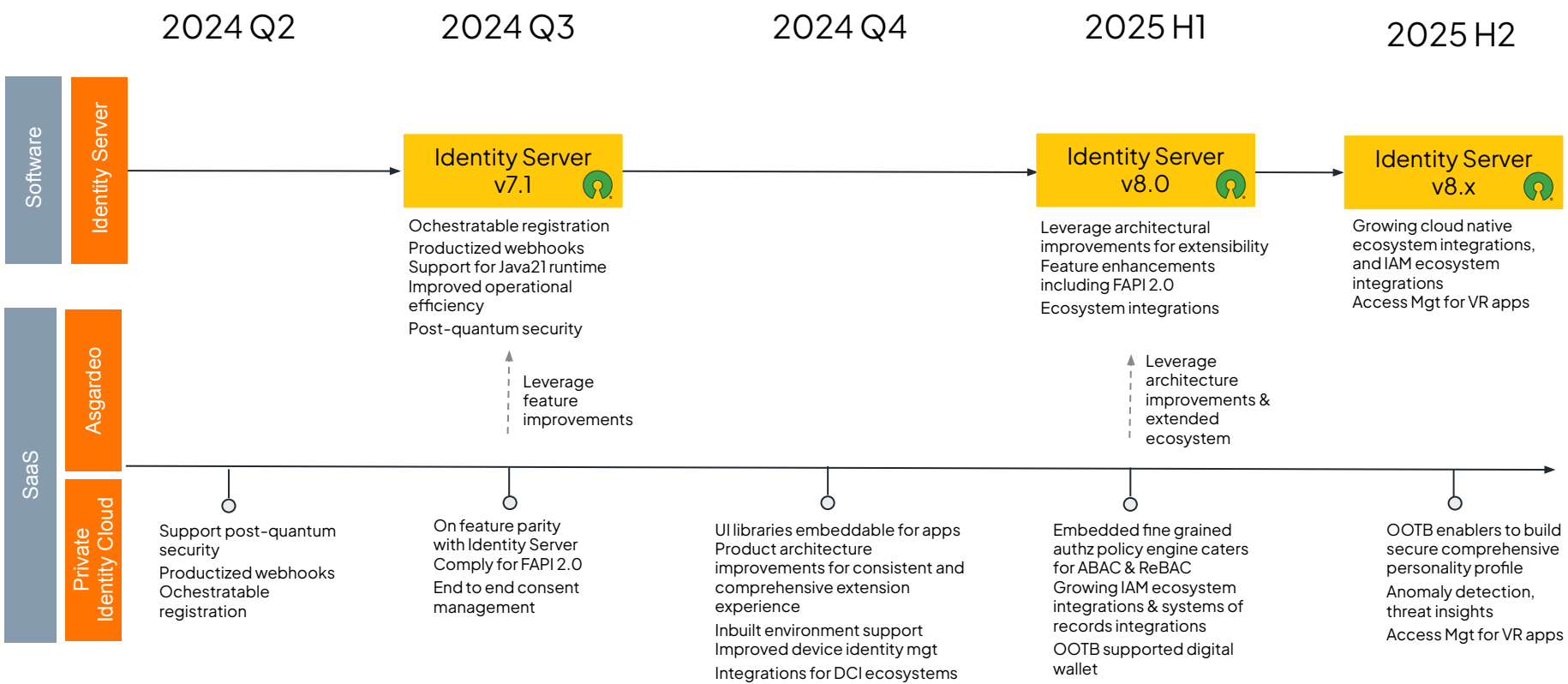
- AI powering the Digital Double (transactions + systems of records + AI)
- Utlized to provide the exceptional digital experiences and secure access
- Should act with consent and control of the user

Identity Theft and Fraud

- AI powering fake Identity
  Deutsche Telekom Deepfake AI Ad*
- Requires identification of reputable/verified services and people to interact
- Strong protection of data
- Stronger requirements for privacy and consent

* Viewer discretion is advised

WSO2 IAM Roadmap – Preparing for Upcoming Advancements



Asgardeo Roadmap

2024 Q2

- Improved UX/DevEx
  - **React, iOS, Flutter SDKs** for **application native login**
- Feature improvements
  - **Registration API closer to OIDC standard** for ochestratable registration flows
  - **Application level branding, ToS** management
  - **Auditing, administrative insights** for **B2B customer admins**
  - **OAuth 2.0 DPoP support**
  - **User impersonation** capabilities to address help desk support use cases
  - Support for **post-quantum security securing internal/external encryption, hashing** with Post Quantum Cryptography (PQC)
- Architecture improvements
  - Productized support for **webhooks for asynchronous communication**
  - **Optimized architecture for operational efficiency:** Redesigned runtime data handling for sessions, Non-persistent tokens, etc.
- Integrations
  - SSO templates for well-know SaaS providers
  - Identity verification: Onfido
  - Facial Biometrics, MFA: iProov, DUO
  - Bot detection: castle.io

2024 H2

- Improved UX/DevEx
  - **Registration, login, progressive profiling, user and IdP management UI libraries** embeddable in applications (2024 Q3)
  - **AI** to simplify building **personalized login experiences** (2024 Q4)
  - **Support for environments** (e.g:dev, stage, prod) with the capability to promote (2024 Q4)
- Feature improvements
  - **FAPI 2.0 compliance** (2024 Q3)
  - Enhanced **fine-grained consent authorization** for business APIs and ability for the end user to **manage authorized consents for third party apps** (On top of RAR, Grant Management) (2024 Q3)
  - Extend **B2B collaboration use cases** where users can collaborate across organizations horizontally or vertically (2024 Q4)
  - Improved **self service** functionalities **to manage device identities** (2024 Q3)
  - Integrate to **Decentralized Credential ecosystem**. 1Kosmos, SpruceID (2024 Q4)
- Architecture improvements
  - Elevating extensibility framework for **consistent and comprehensive extension experience** with refined scripting at login, registration and account management flows
  - Add **custom authentication, invoking custom code** deployed in Choreo
- Integrations (2024 Q3-Q4)
  - Consent management: OneTrust, DataGuard
  - Identity verification :Trusona, Keyless
  - Bot/fraud detection:Sift, Imperva, LexisNexis
  - Authorization : Axiomatics, Styra

2025+

- **Authorization policy engine** enhancement supporting RBAC, ABAC & ReBAC
- **Security monitoring** and **data visualization dashboards**
- Build a **comprehensive personality profile** with interactions, transactions and omnichannel activities
  - Master data management and integrations with systems of record
  - **APIs for querying the personality, patterns and classifications** to build personalized experiences
  - Event processing and **AI/ML** analysis of all data **to derive insights** on behalf of businesses
  - **Triggers** alerting anomalies and transactions
- **Digital wallet** compliant with **EU digital wallet** and **Open Wallet** specification
- **Access Management** on **VR apps** (metaverse, vision-os)
- Continued ecosystem supporting,
  - PAM, IGA
  - Adjacent business system integrations CMS, web3
  - Decentralized identity and integrations with intelligent IDVs, Synthetic identity fraud detection

WSO2 Identity Server Roadmap

2024 H2

- Improved UX/DevEx
  - Build **login/registration flows with natural language input utilizing LLMs**
  - **AI to automate** end user facing UI/email **branding** to match applications look and feel
  - **React, Android, iOS, Flutter SDKs** for **application native login**
- Feature improvements
  - **Registration API closer to OIDC standard** for ochestratable registration flows
  - **Application level branding, ToS** management
  - **OAuth 2.0 DPoP** support
  - Extend **B2B collaboration use cases** where users can collaborate across organizations horizontally or vertically
  - **User impersonation** capabilities to address help desk support use cases
  - Support for **post-quantum security securing internal/external encryption, hashing** with Post Quantum Cryptography (PQC)
- Architecture improvements
  - Elevating extensibility framework for **consistent and comprehensive extension experiences** with refined scripting, events, and webhooks
  - **Optimized architecture for operational efficiency:** Redesigned runtime data handling for sessions, Non-persistent tokens, etc.
- Integrations
  - SSO templates for well-know SaaS providers
  - Identity verification: Onfido
  - Facial Biometrics: iProov
  - Bot detection: castle.io

2025 H1

- Improved UX/DevEx
  - **Registration, login, progressive profiling, user and IdP management UI libraries** embeddable in applications
  - **AI** to simplify building **personalized login experiences**
  - **Support for environments** (e.g:dev, stage, prod) with the capability to promote
- Feature improvements
  - Enhanced **fine-grained consent authorization** for business APIs and ability for the end user to **manage authorized consents for third party apps** (On top of RAR, Grant Management)
  - Improved **self service** functionalities **to manage device identities**
  - **FAPI 2.0 compliance**
  - **User impersonation** capabilities to address help desk support use cases
- Integrations
  - Identity verification: Trusona, Keyless
  - Consent management: OneTrust, DataGuard
  - Bot/fraud detection: Sift, Imperva, LexisNexis
  - Authorization : Axiomatics, Styra

2025 H2+

- **Authorization policy engine** enhancement supporting RBAC, ABAC & ReBAC
- Agents and enablers to build a **comprehensive personality profile** with integrations for Master data management and systems of record
  - **APIs for querying the personality, patterns and classifications** to build personalized experiences
- **Access Management** on **VR apps** (metaverse, vision-os)
- Continued ecosystem supporting,
  - PAM, IGA
  - Adjacent business system integrations CMS, web3
  - Decentralized identity and integrations with intelligent IDVs, Synthetic identity fraud detection

Thank You!

Managing access for a Single Page Web Application

- Integrate with Asgardeo
- Self registration
- Account linking
- Self service account management
- Multi-Factor Authentication (MFA)
- Passwordless Authentication
- Access a high assurance API
- Integrate with Salesforce

```
import React from "react";
import { render } from "react-dom";
import { AuthProvider } from "@asgardeo/auth-react";

const Index = () => (
    <AuthProvider
        config={ {
            signInRedirectURL: "http://localhost:3000",
            signOutRedirectURL: "http://localhost:3000",
            clientID: "owH7CxjRkazFD0PnTwENNkWwAC8a",
            baseUrl: "https://dev.api.asgardeo.io/t/intdemo",
            scope: [ "openid","profile" ]
        } }
    >
        { /* Rest of your application.  */ }
    </AuthProvider>
);

render((<Index />), document.getElementById("root"));
```