20TH ANNIVERSARY EDITION

WSO2CON ASIA

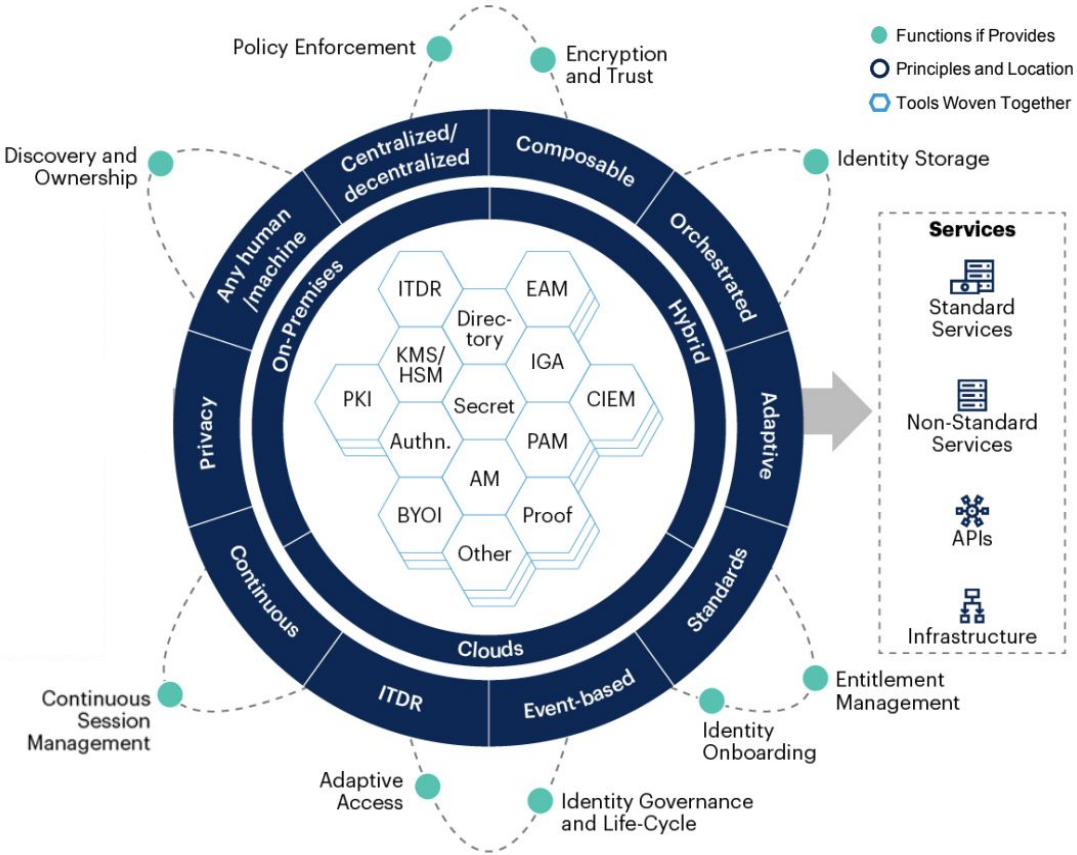
PLATFORMLESS MODERNIZATION

Map your Enterprise IAM Needs to a Reference Architecture



Johann Dilantha Nallathamby
Head of Solutions Architecture - IAM
WSO2

IAM is a Composition!!



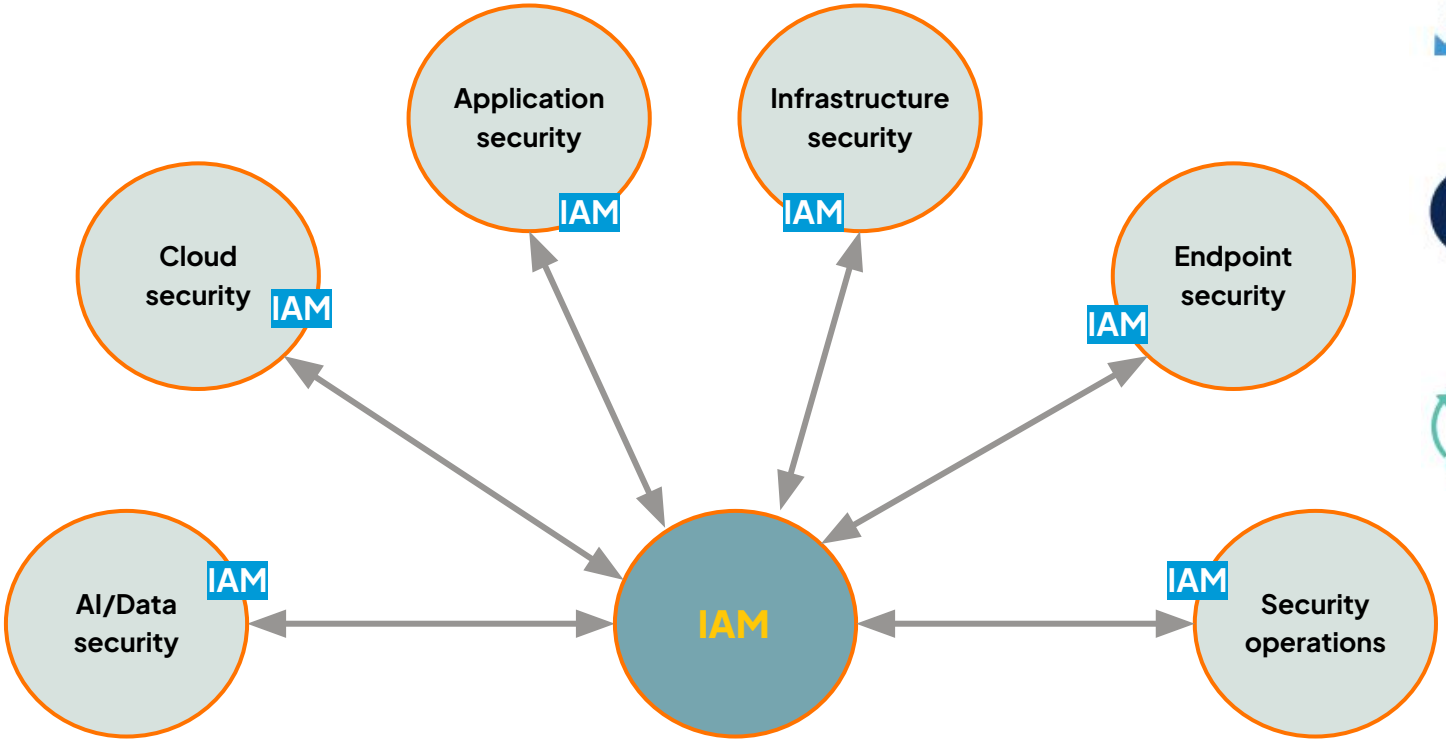
*Source: Identity Fabric – The Definition and its Architecture – Felix Gaehtgens, Gartner IAM Summit 2024, London

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

- Gartner -



Identity-first Security



Consistent

Context-aware

Continuous

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

- Gartner -



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

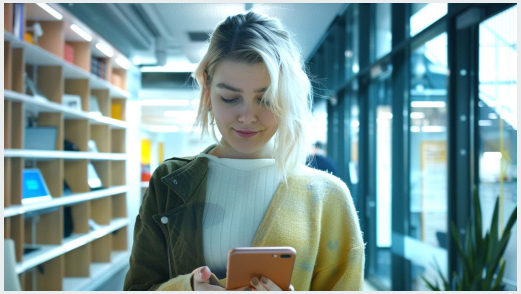


- OAuth 2.0/OIDC compliance
- Consent-, role- and context-based authorization
- Pre-integrated API gateways

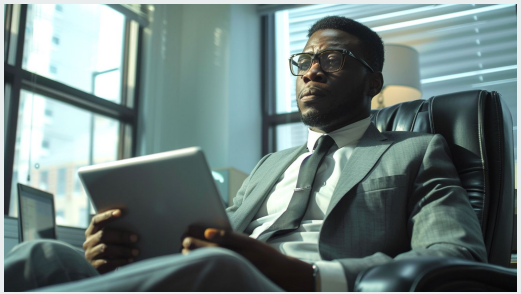
All Users Deserve Seamless and Secure Digital Experiences

Identity and Access Management

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







Background

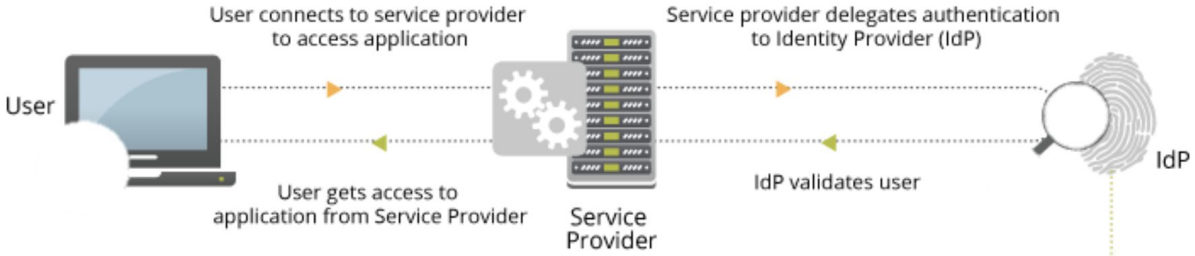
Traditional Applications

- Basic authentication
- Digest authentication
- Client-cert authentication
- Form based authentication

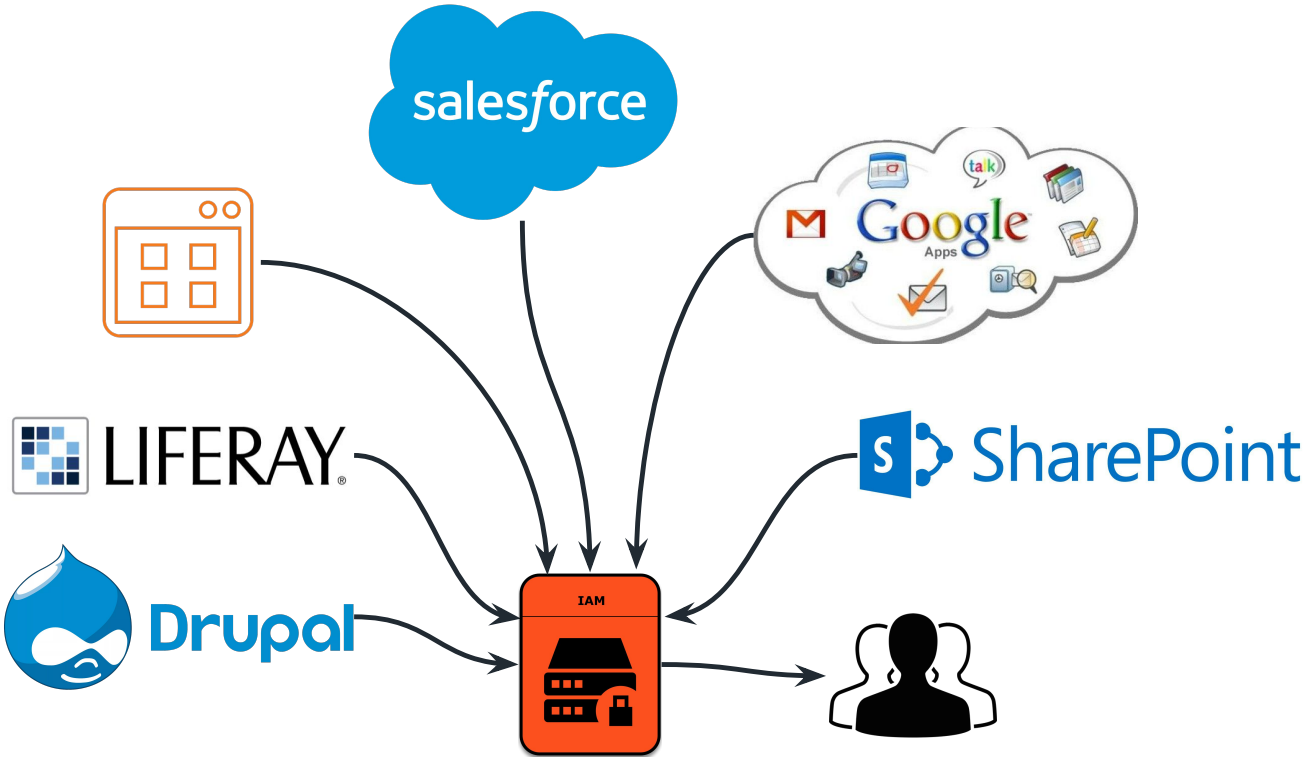
Traditional vs. Modern Applications

Traditional	Modern
Identity silos	Identity broker
Monolith	Service Oriented Architecture
Broad access	Fine-grained access
No data sharing	Data sharing

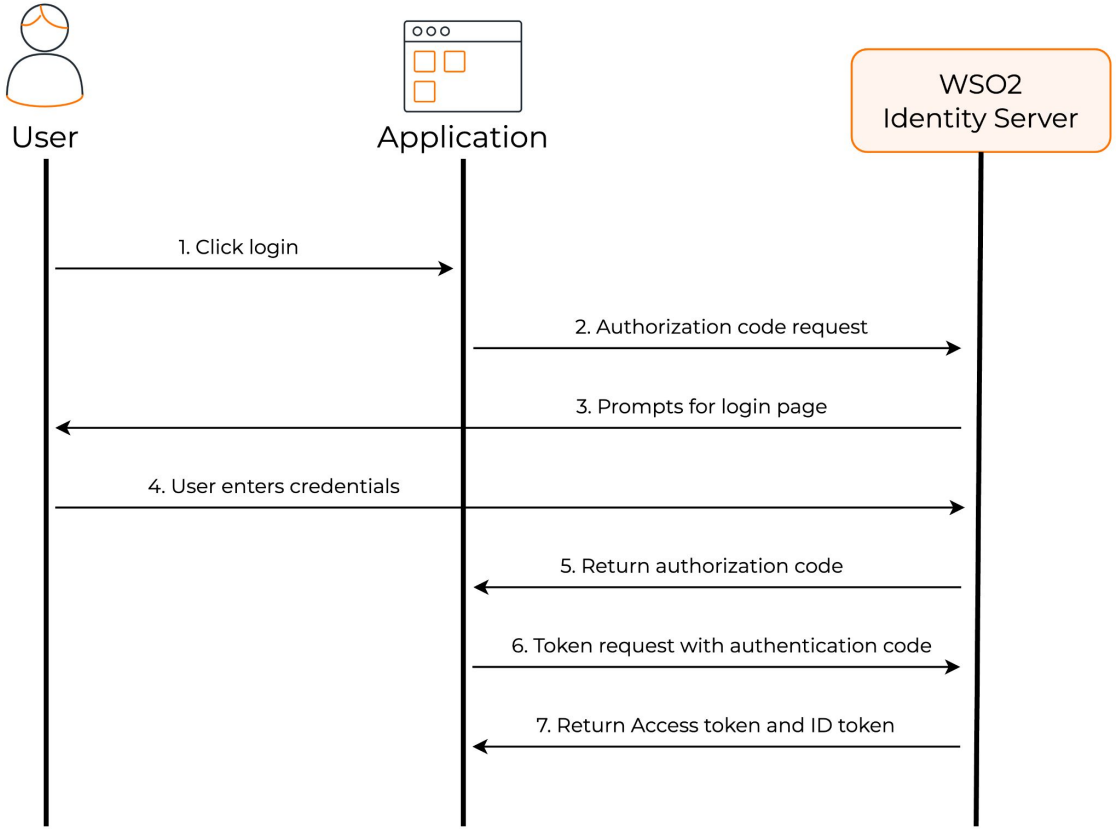
Identity Brokering



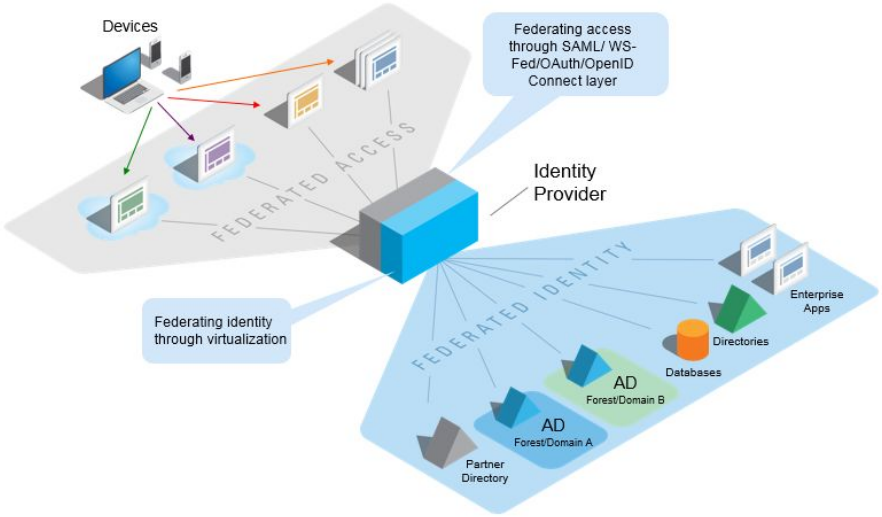
Identity Brokering



OpenID Connect Authorization Code Login

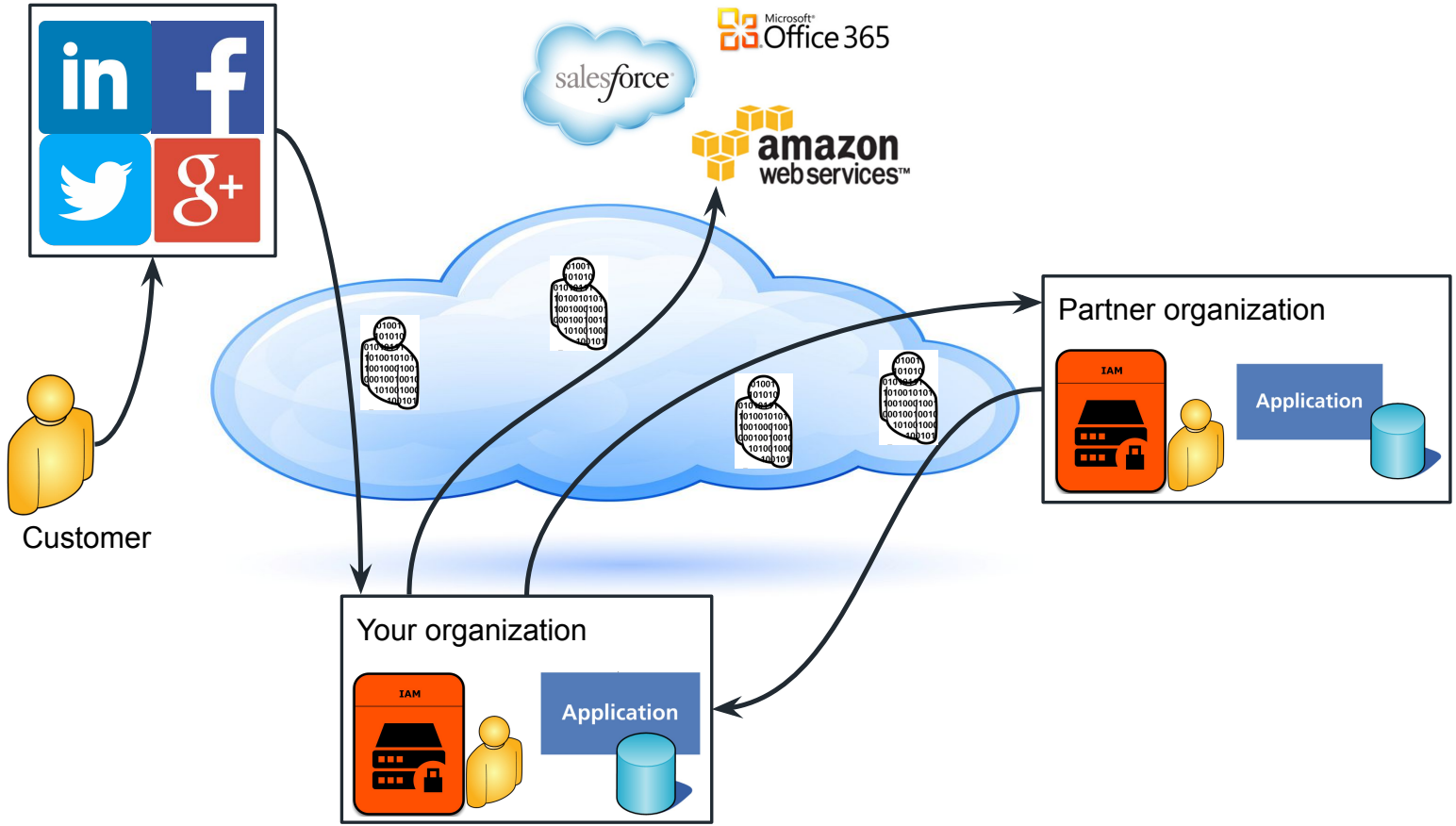


Federated Identity

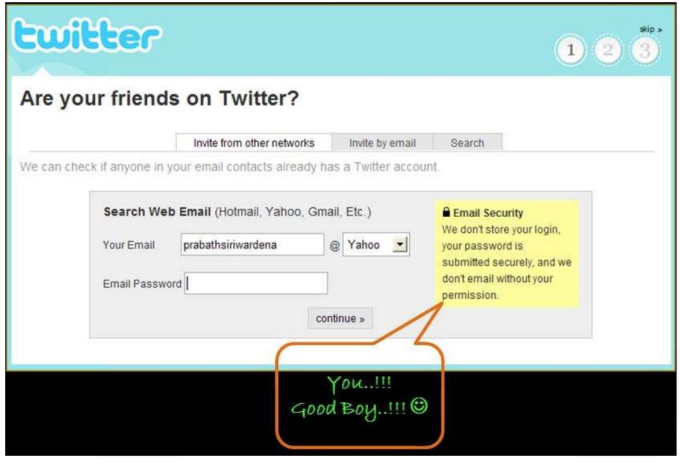


Granting access to identities that are managed in different identity silos

Federated Identity



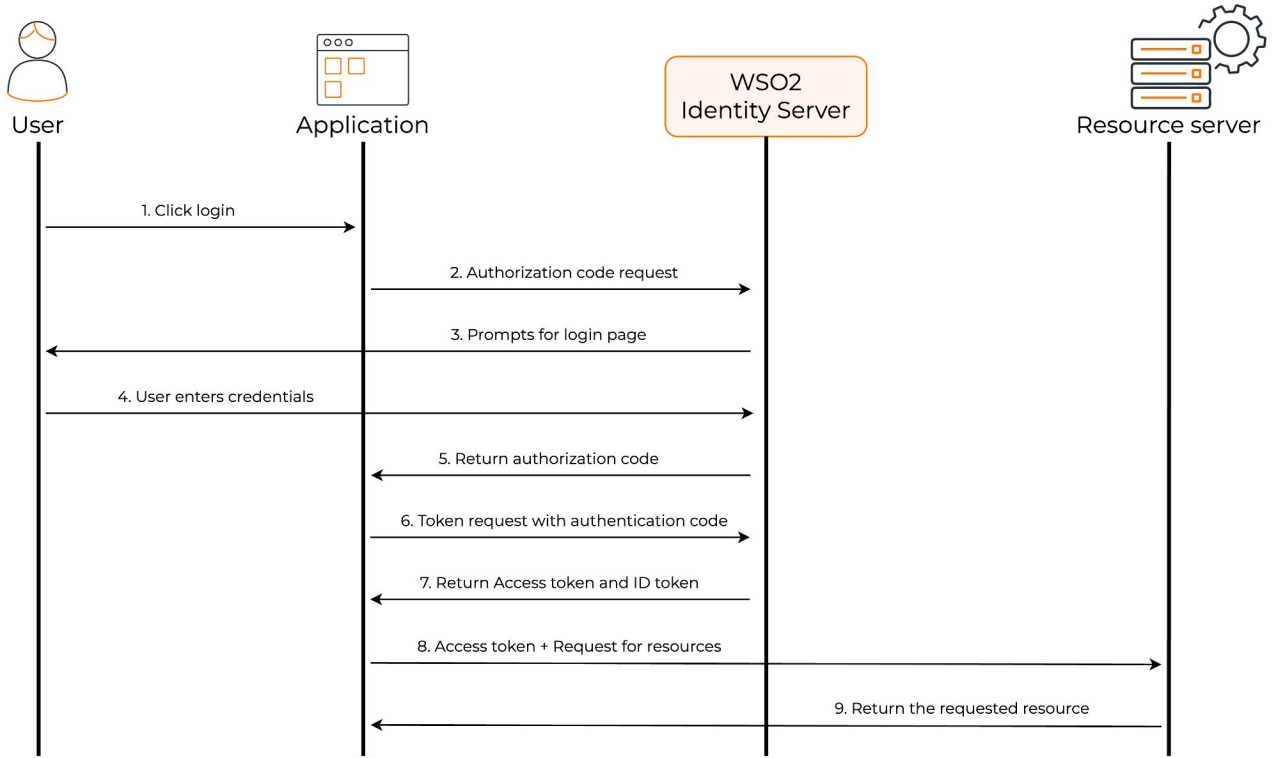
Data Access


twitter
skip »
1 2 3
Are your friends on Twitter?
Invite from other networks
Invite by email
Search
We can check if anyone in your email contacts already has a Twitter account.
Search Web Email (Hotmail, Yahoo, Gmail, Etc.)
Your Email
prabathsiriwardena
@ Yahoo
Email Password
continue »
Email Security
We don't store your login, your password is submitted securely, and we don't email without your permission.
You..!!!
Good Boy..!!!


Make sure you do a blog post everyday.. Hah...
slideshare
Hello, guest!
Home
Browse
My Slidespace
Upload
Community
Tags
Widgets
Latest
Most Viewed
Most Embedded
Featured
Most Favorited
Most Downloaded
Slidecasts
Post to Twitter
Post to Blogger:
Blogger username:
Title:
Blogger password:
Post to sidebar
Post

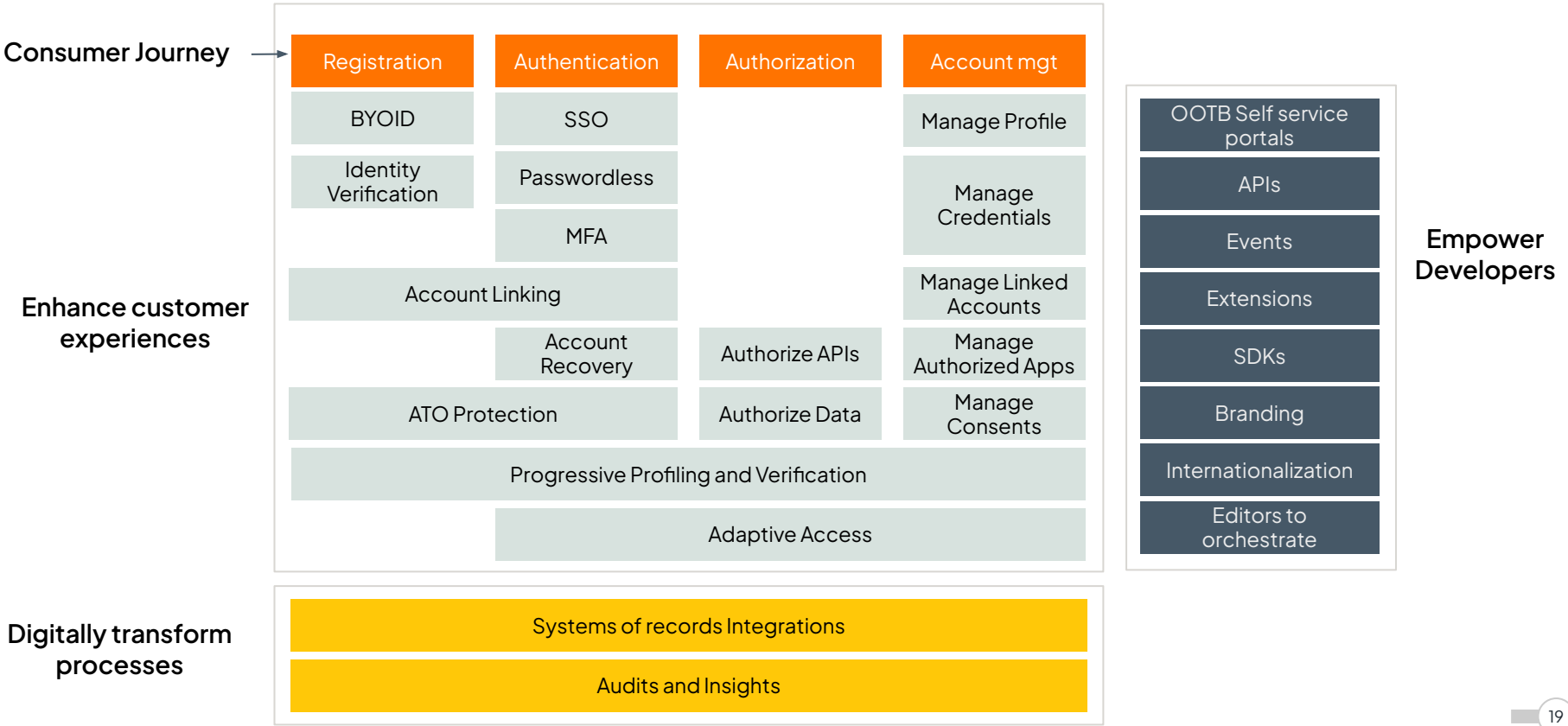

Find your friends on hi5
hi5
CHECK YOUR ADDRESS BOOK
Email Address:
prabathsiriwardena
@ gmail.com
Email Password:
Find Friends
...or find friends by their email addresses
We don't store your email and password information or contact your friends without your permission.

OAuth 2.0 Authorization Code Grant Flow



IAM for Consumers and Employees

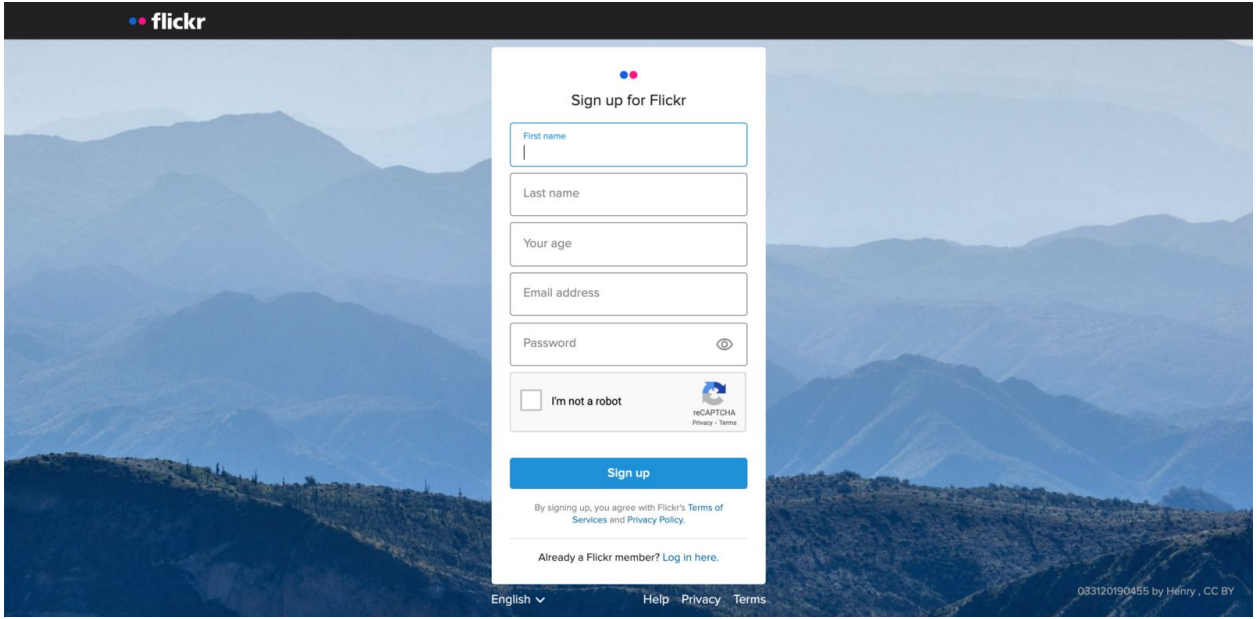
Critical Capabilities for Consumer and Employee IAM



Onboarding

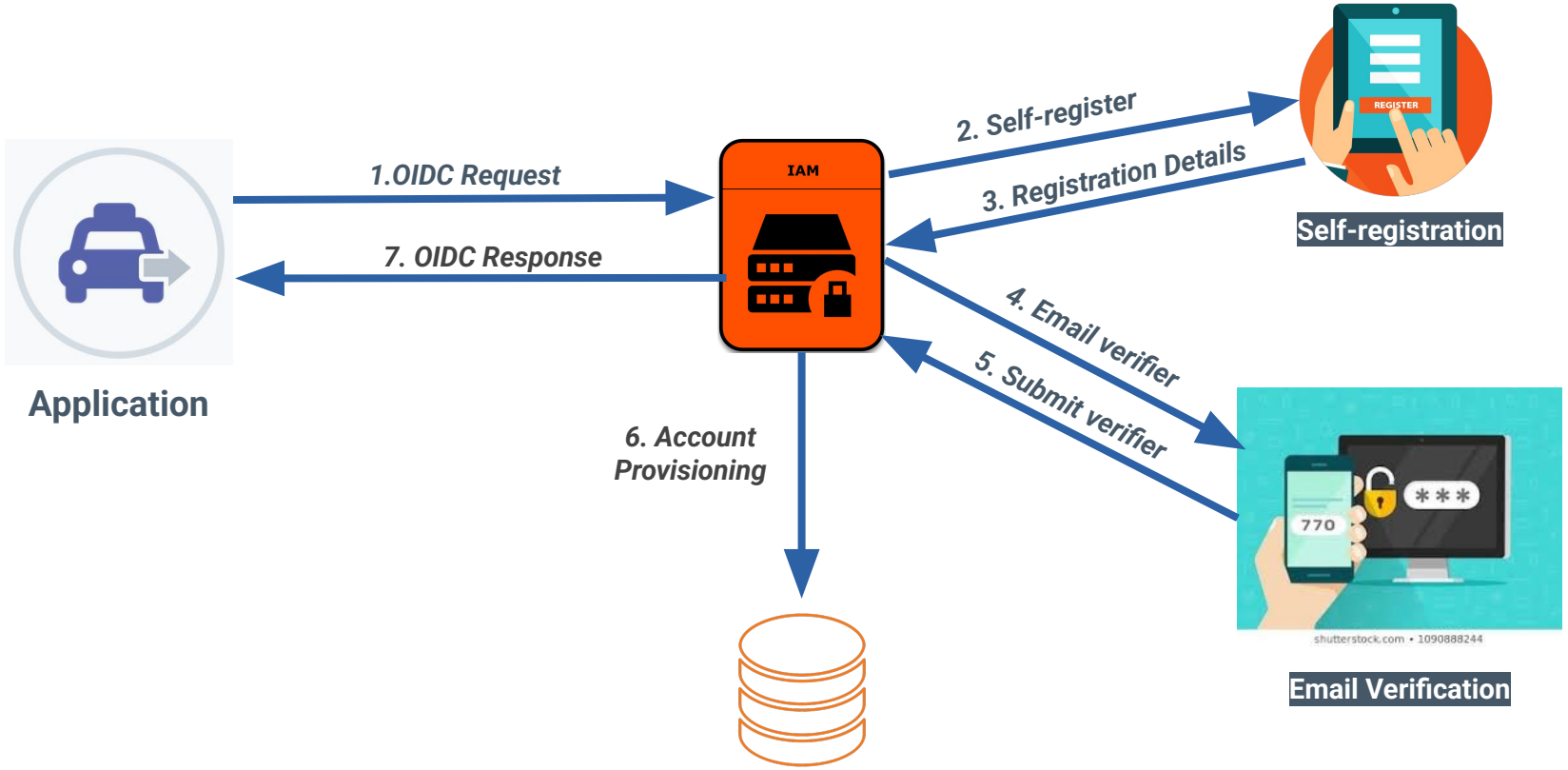
Self-registration

End-consumer initiates a request to provision an account for him/her in the system by providing his/her details.



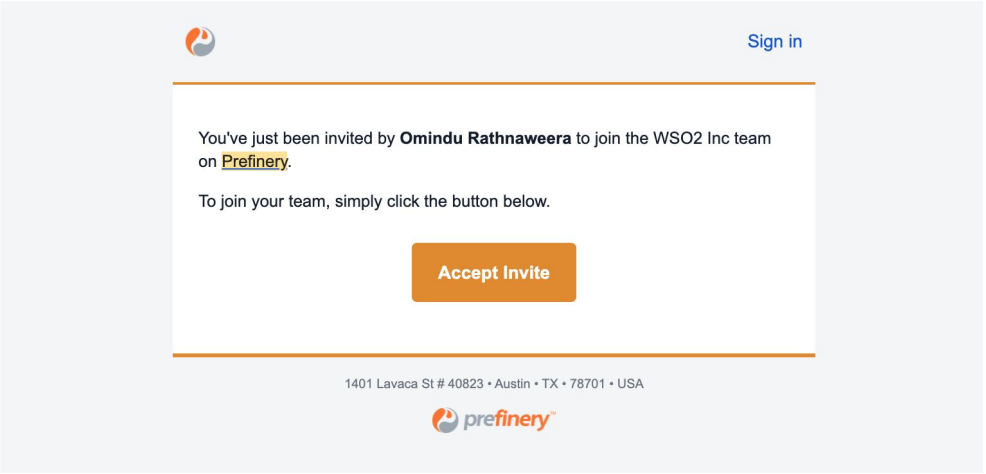
Self-registration in Flickr

Self-registration + Email verification



Invitation

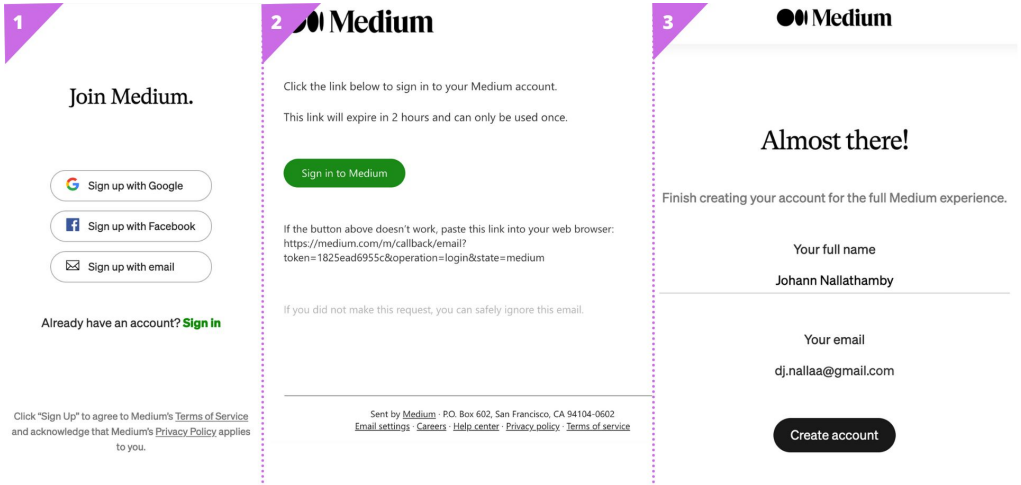
Administrator, with the relevant authorization within the organization, initiates a request to provision a consumer account, which, in turn, sends out an invite to the consumer's verified 2-factor authentication (2FA) channel, such as a verified email address or verified mobile number.



Invitation Workflow in Prefinery for Enterprises

Just-In-Time Provisioning

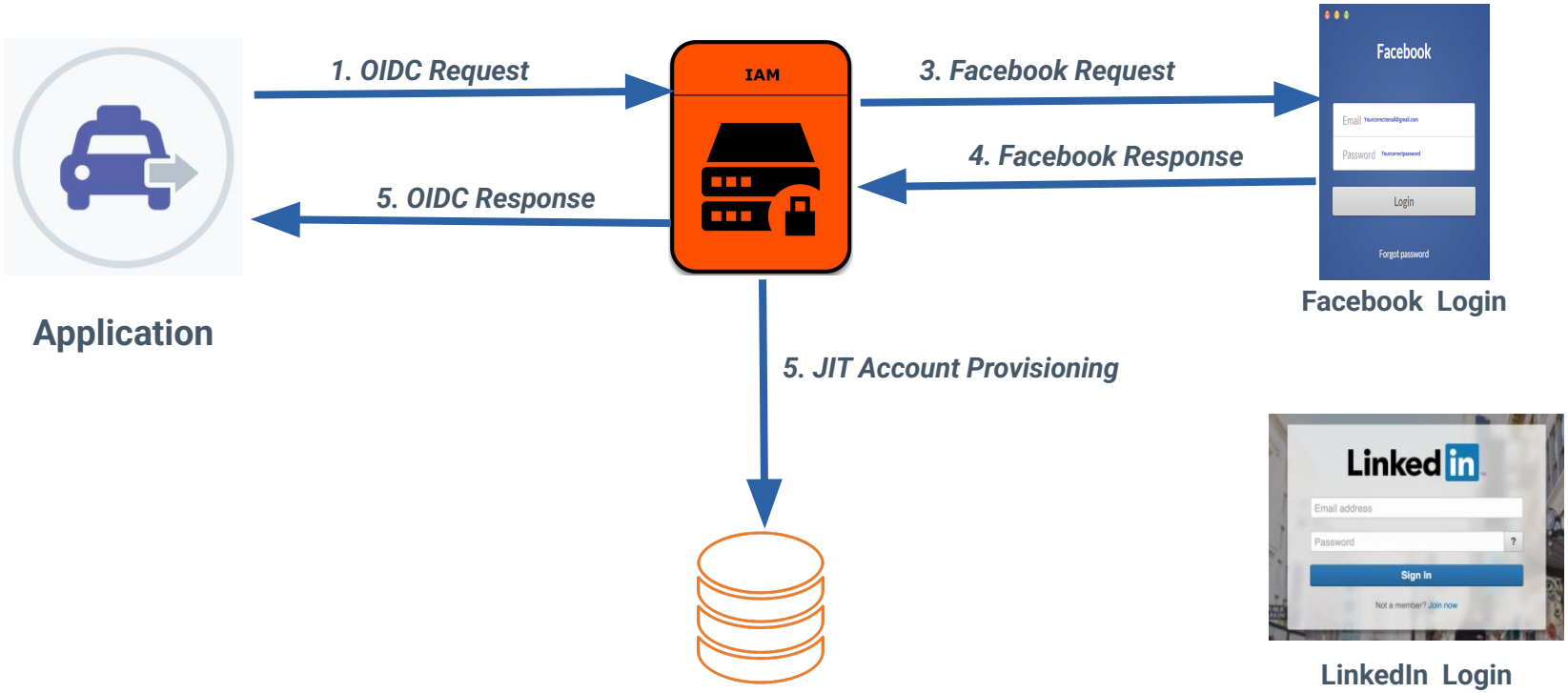
The end-consumer initiates a *federated log-in* [1] as part of which an account is provisioned in the system.



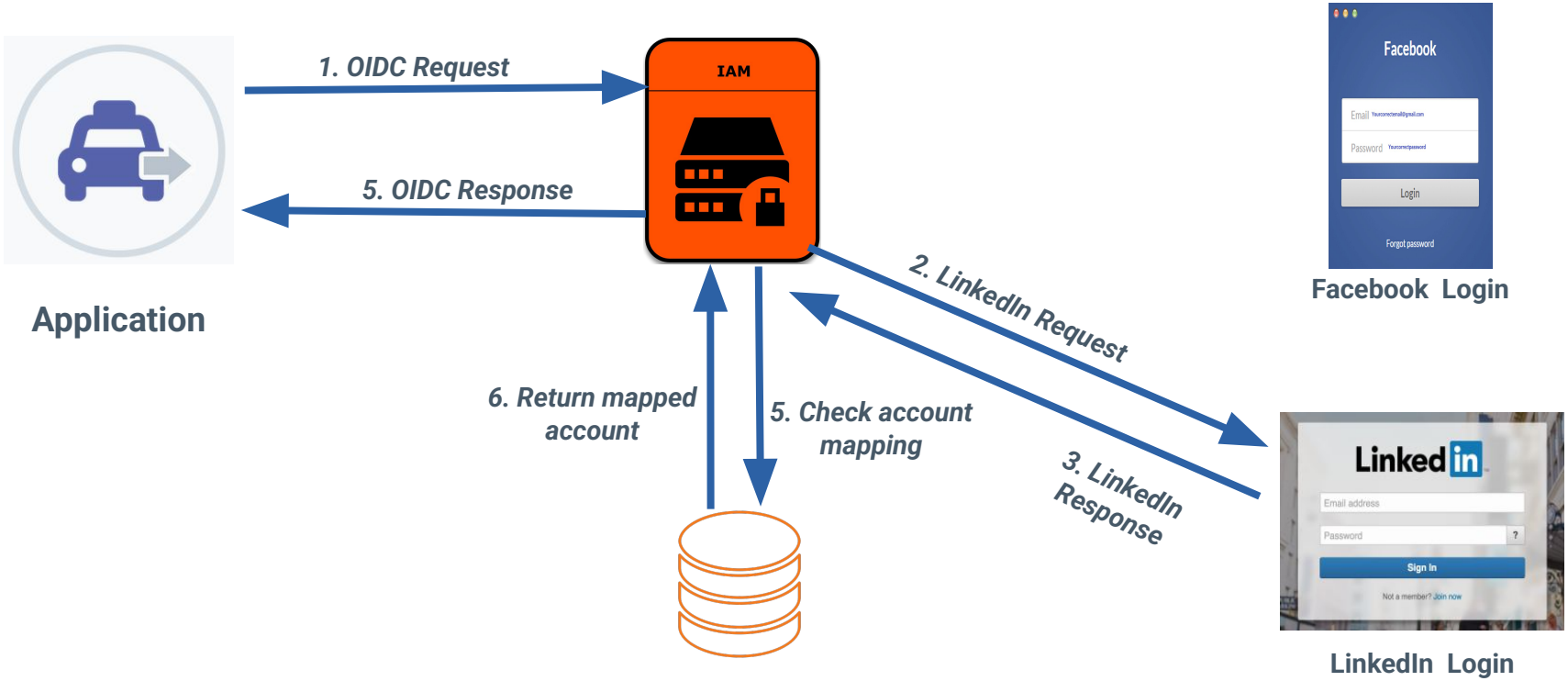
Just-In-Time Provisioning Workflow using Facebook Login in Medium

https://johann-nallathamby.medium.com/federated-identity-management-38b97b690788

Social Sign-up



Social Sign-up



Federated Account Linking Policies

Implicit Linking

Link that are suggested through rules, requiring further verification to confirm.

Explicit Linking

Link that is stated directly and clearly, leaving no room for doubt or confusion.

Implicit Linkage Policies

- Link based on a match between a combination of one or more verified claims asserted by the federated identity provider and independently verified by the resident identity provider.

  E.g. matching verified email addresses, mobile numbers, etc.

- Interactive account linking

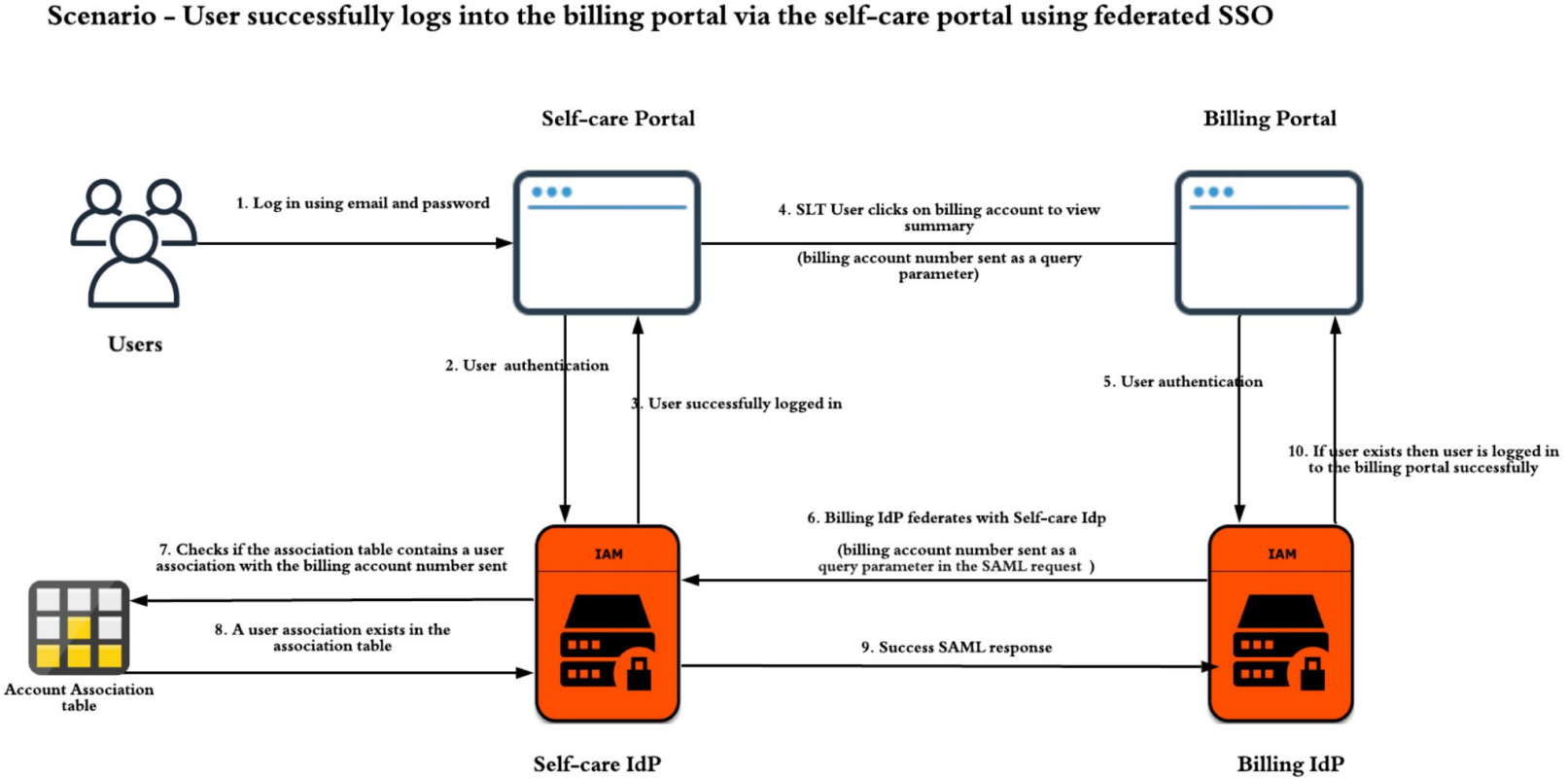
  Link based on the federated assertion and independently proving ownership of the local account in the resident identity provider

Explicit Linkage Policies

- Automatic/silent linking for just-in-time provisioned accounts

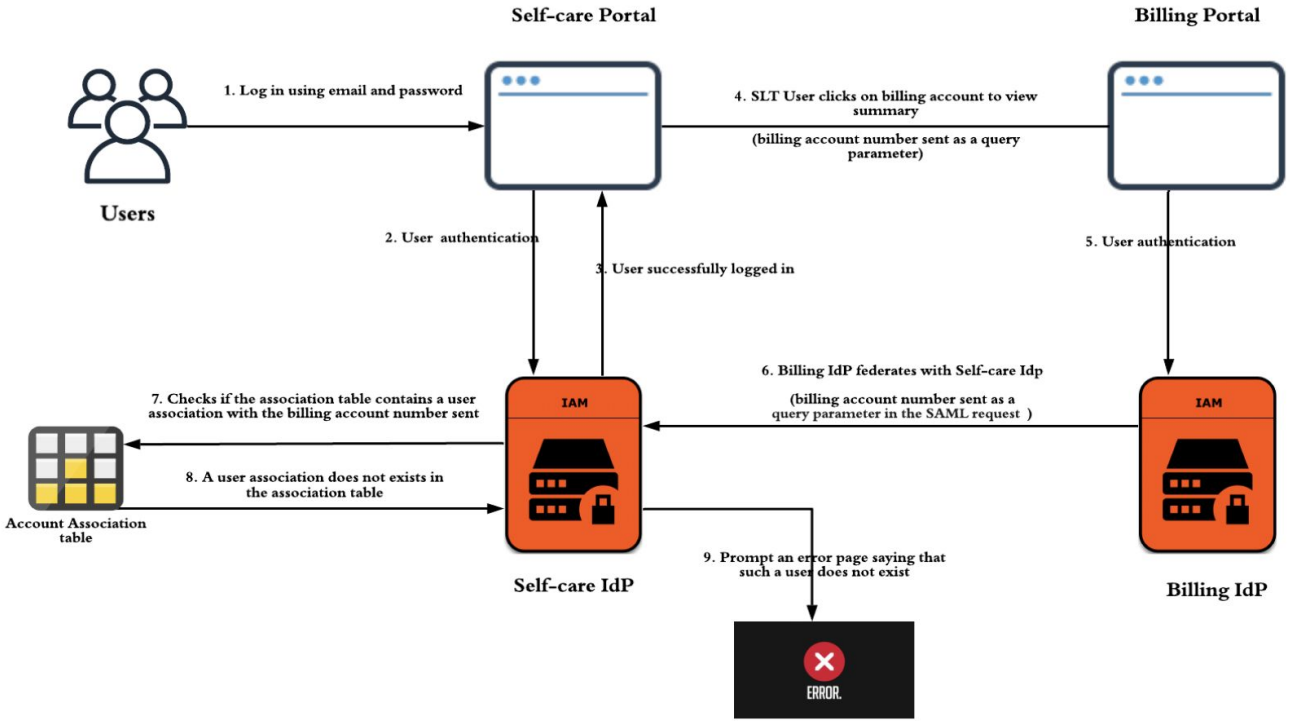
- Link based on external knowledge
  - Outside the scope of the identity broker
  - Usually defined by administrator

Example: Link based on External Knowledge

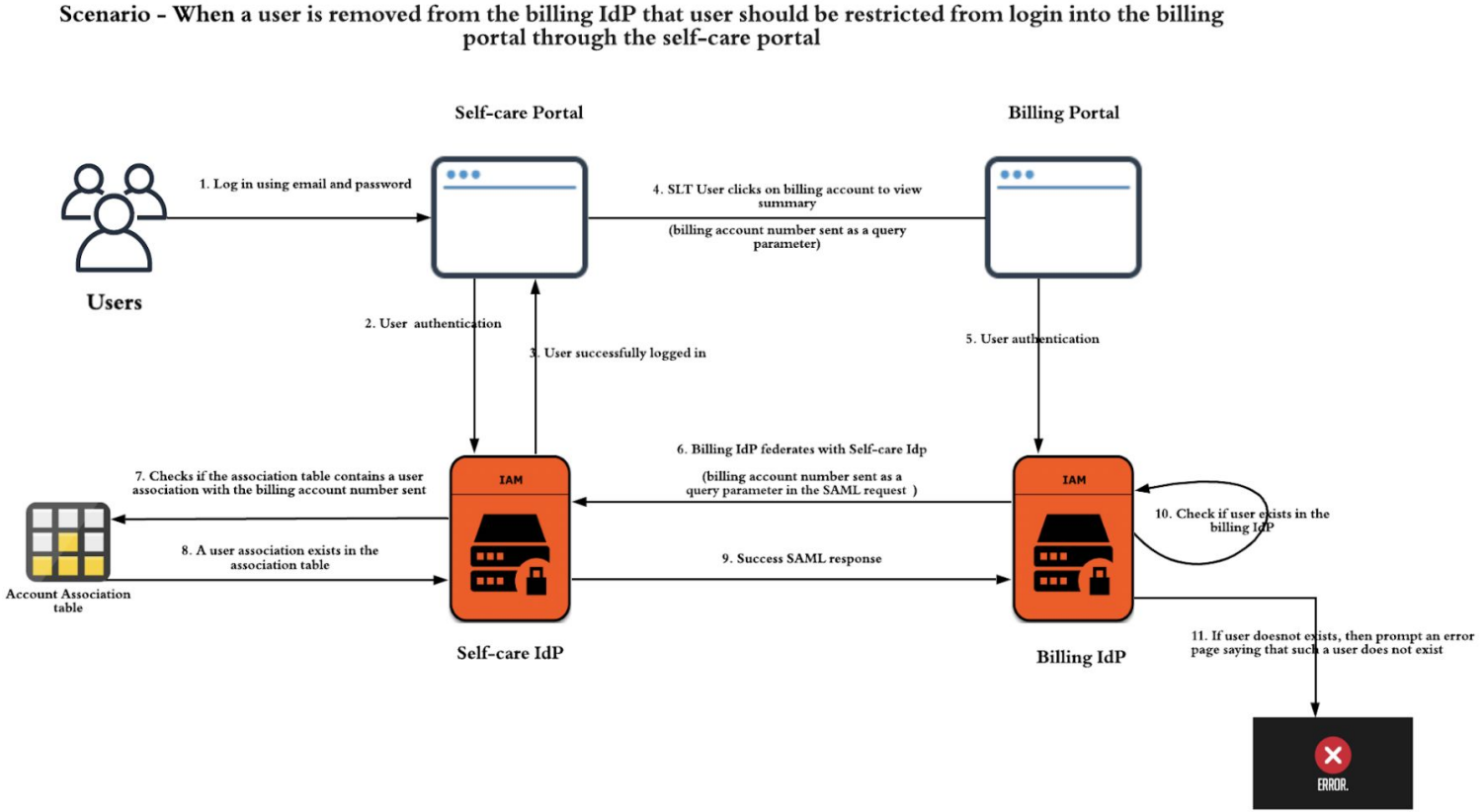


Example: Interactive Account Linking

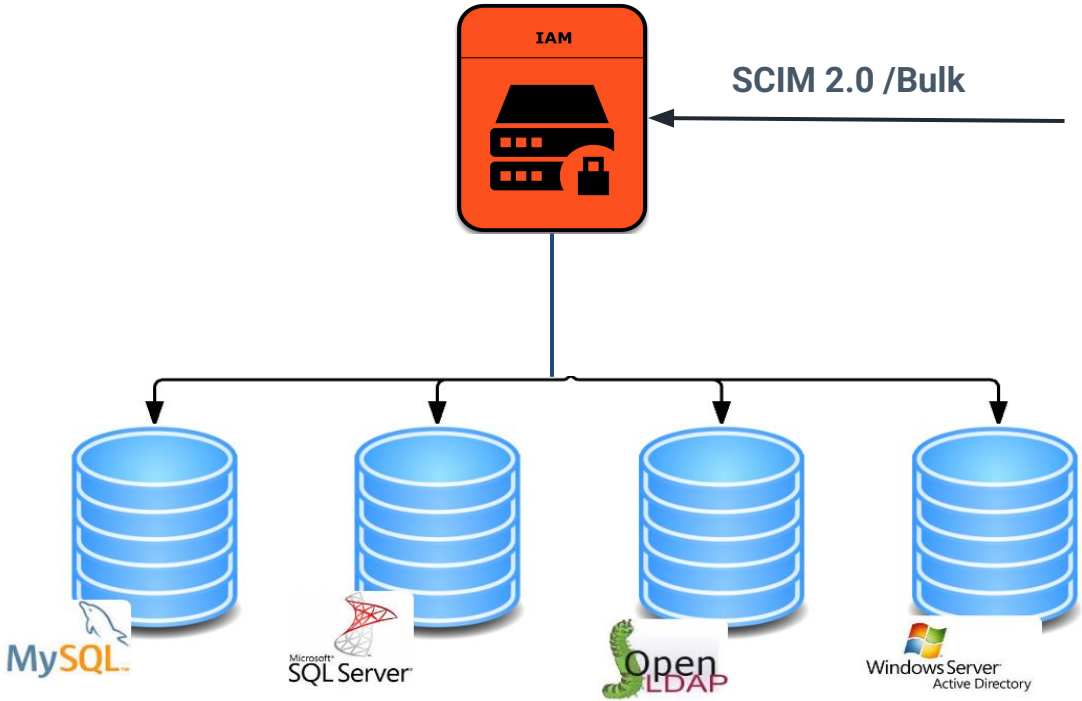
Scenario – If there's a user in the billing IdP whose association is not defined in the self-care IdP direct the user to an error page



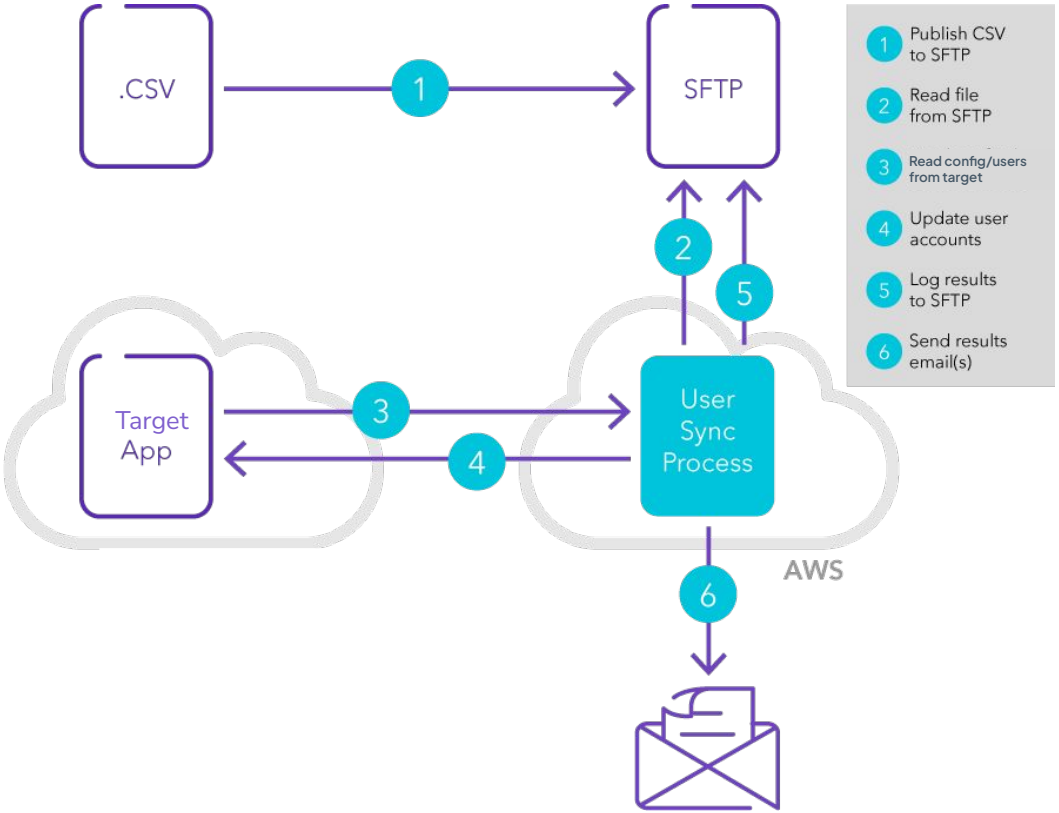
Example: Billing Account Validation



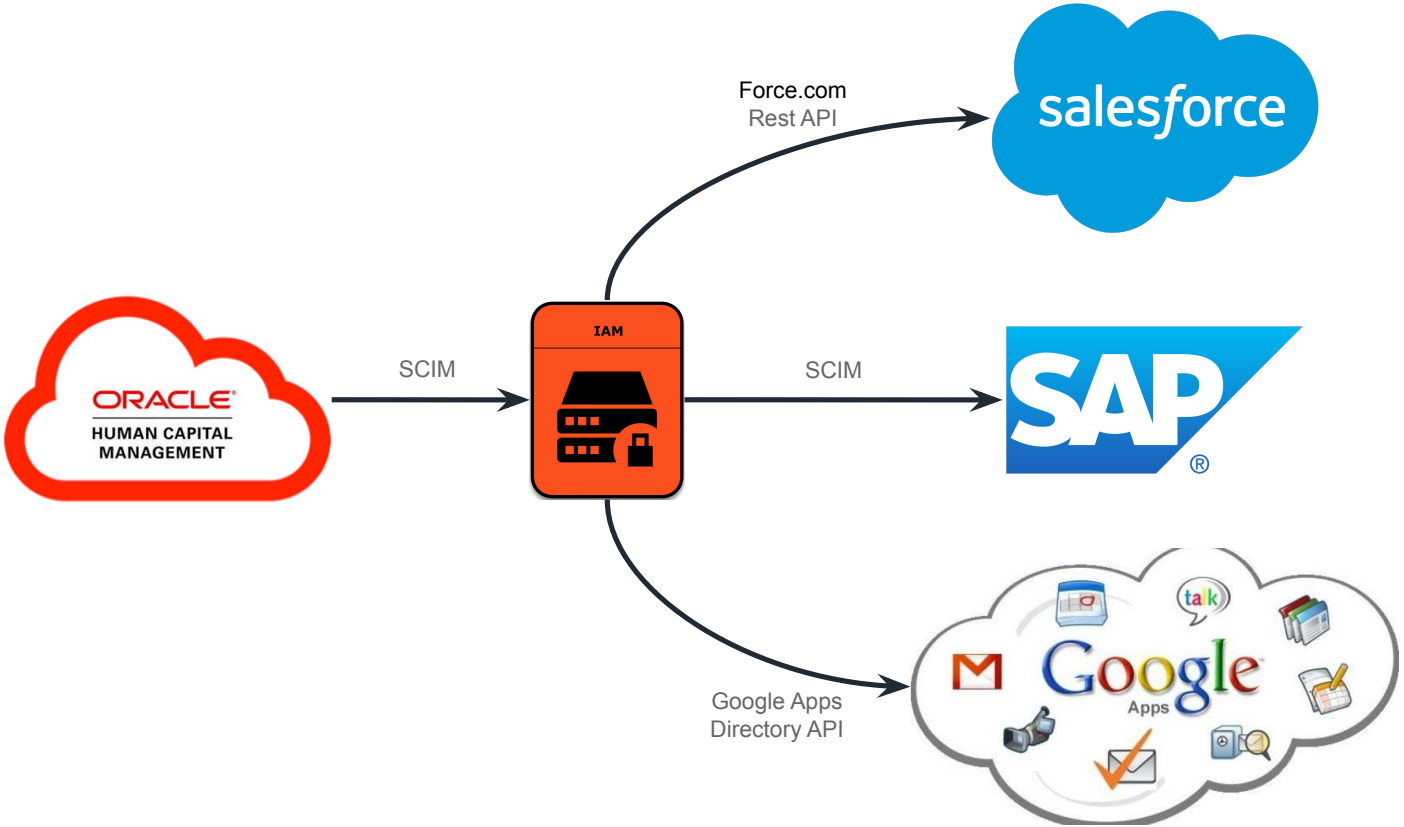
Directory Integration / SCIM 2.0 Bulk



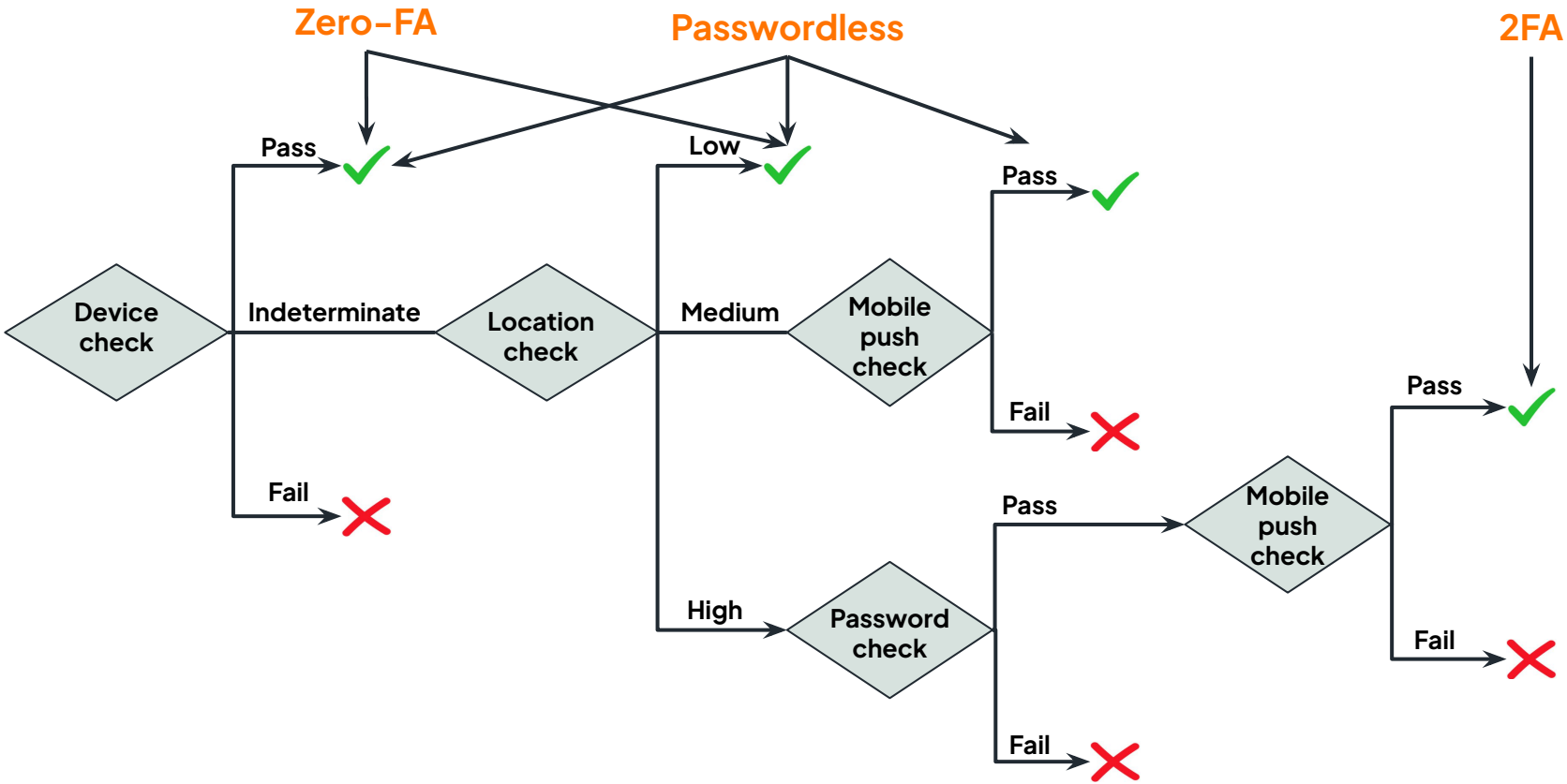
Bulk Onboarding – User–Sync Process



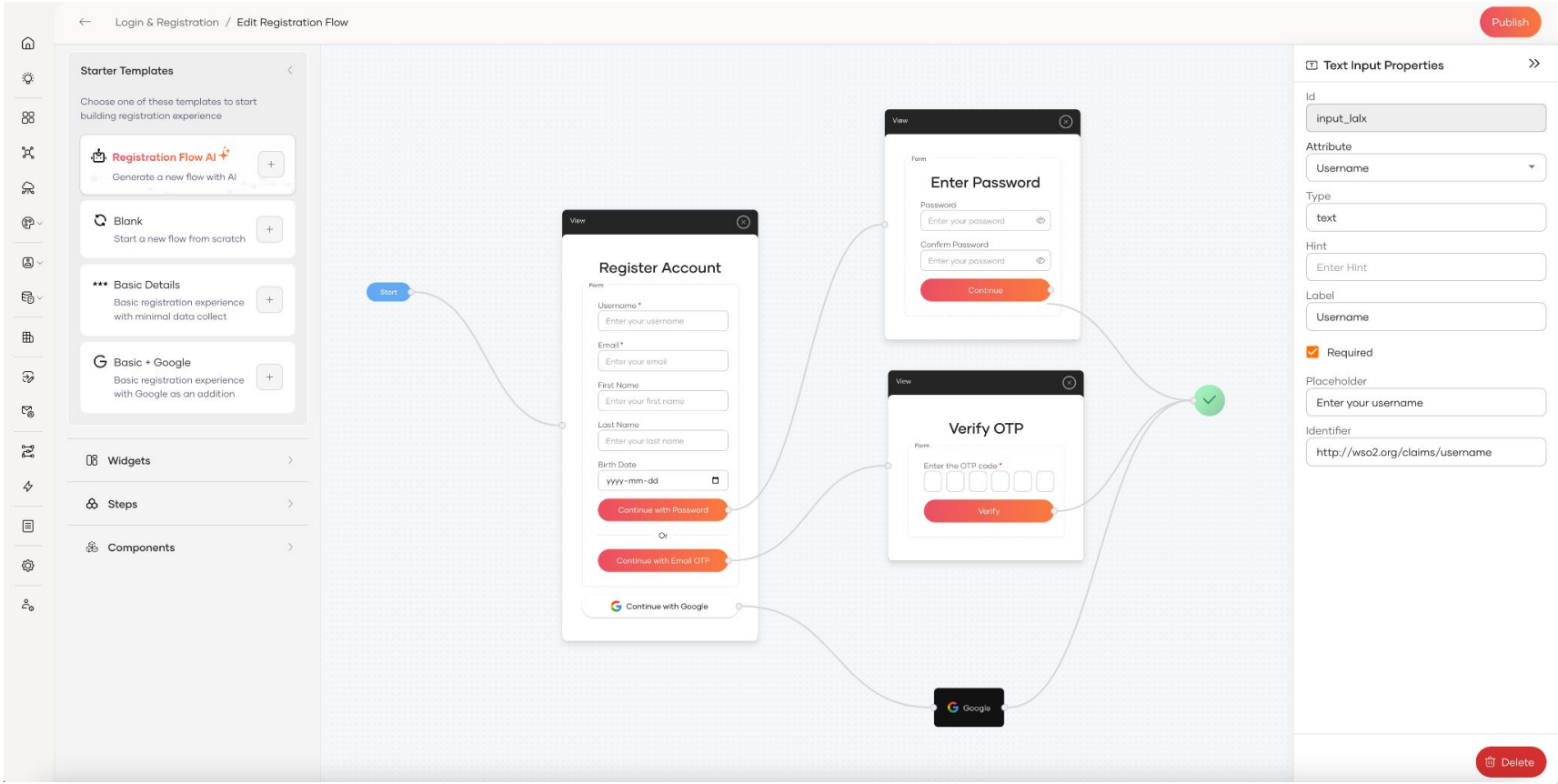
Identity Synchronization



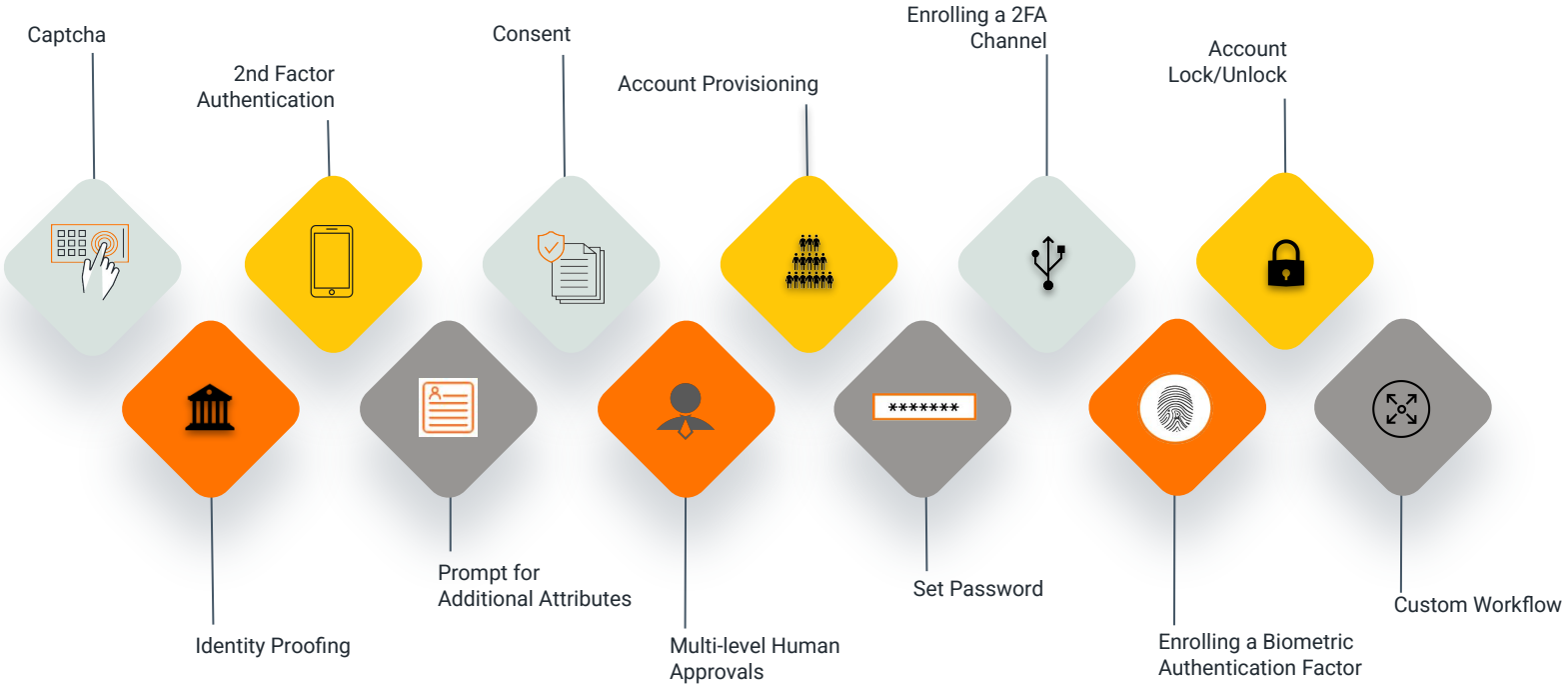
IAM is a Journey-time Orchestration



Democratization of IAM

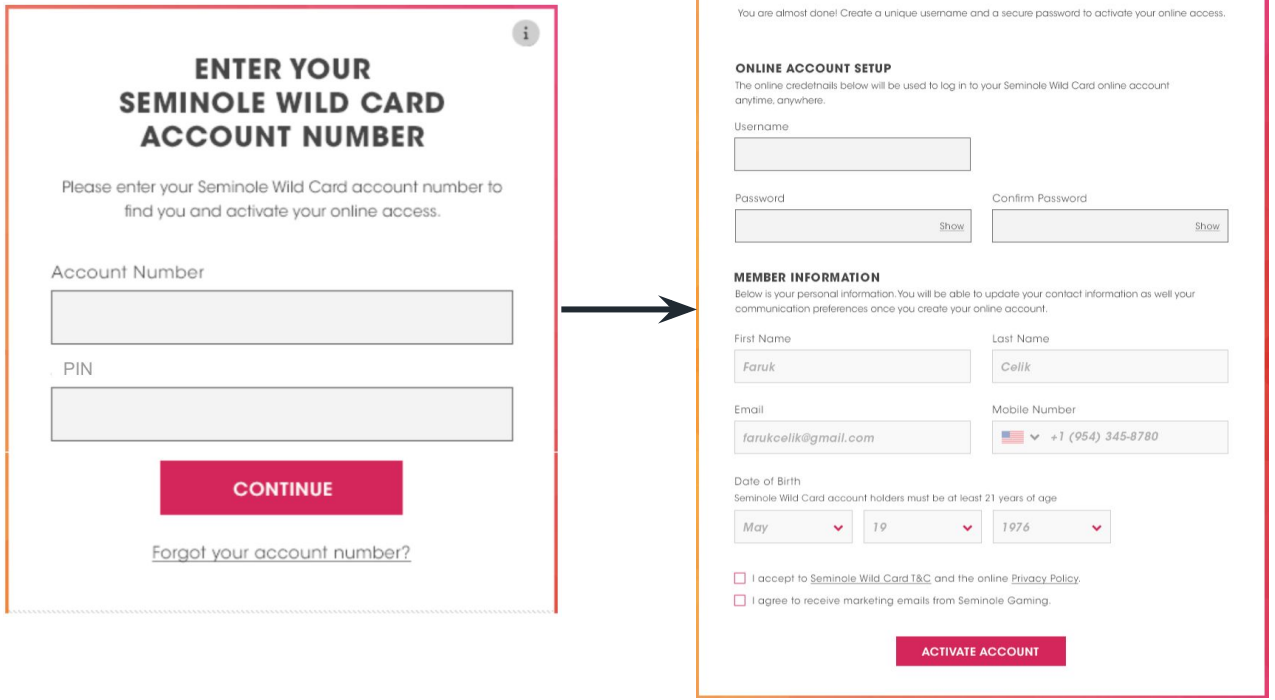


Consumer Onboarding Workflow Components



Identity Proofing

Knowledge-based identity proofing



Identity Proofing

Document verification + Biometrics based Identity Proofing



Customer is asked to scan their ID document



ID is authenticated against security features



Customer facial image is compared with face in ID document

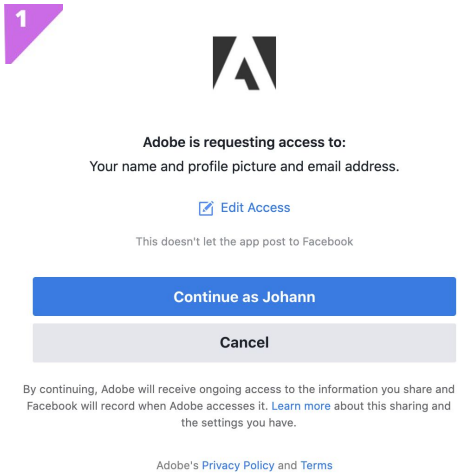


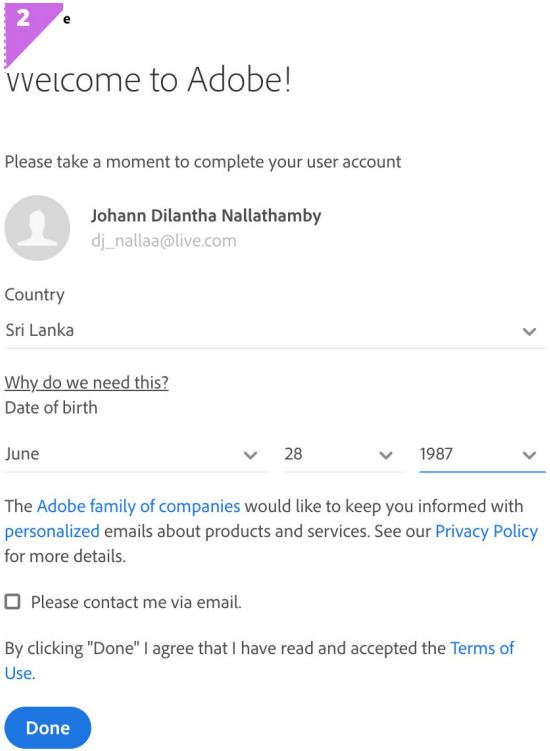
Biometric facial recognition ensures the person is actually present.

Consumer Onboarding Workflow Components

Prompt for Additional Attributes

Authenticating and ensuring that the user who is interacting with the system is in fact the legitimate consumer who he/she claims to be.





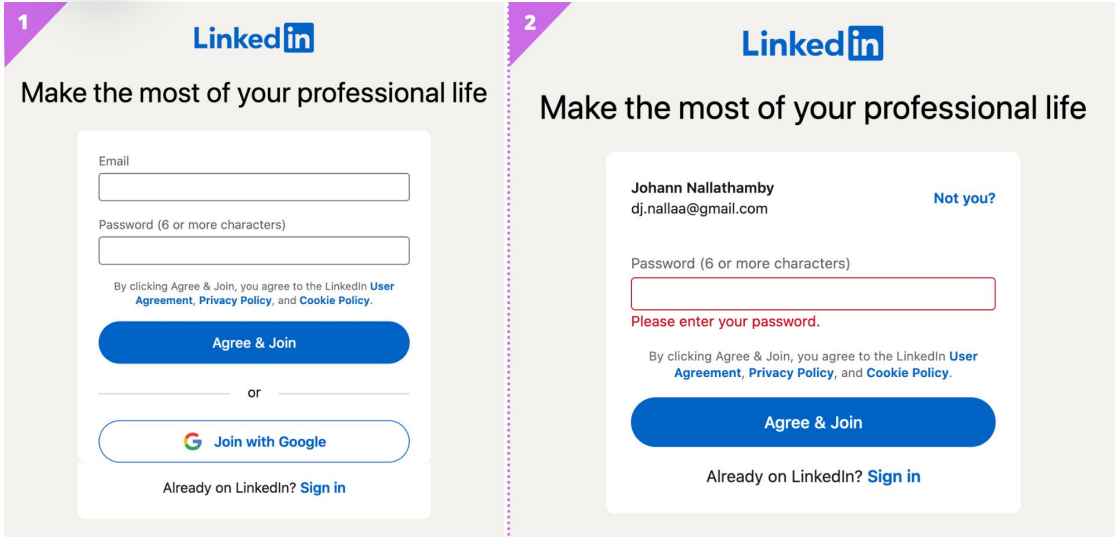
Just-In-Time Provisioning using Facebook Login in Adobe Spark - Date-of-Birth collected from the Consumer

Consumer Onboarding Workflow Components

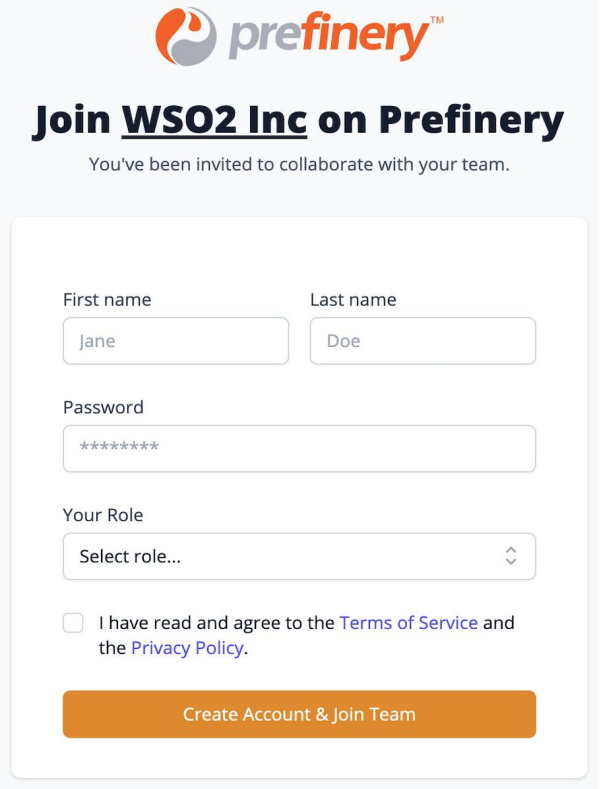


Set Password

Prompts the consumer for a new password and sets it to his/her account



Just-In-Time Password Provisioning using Google Login in LinkedIn - New Password Prompted

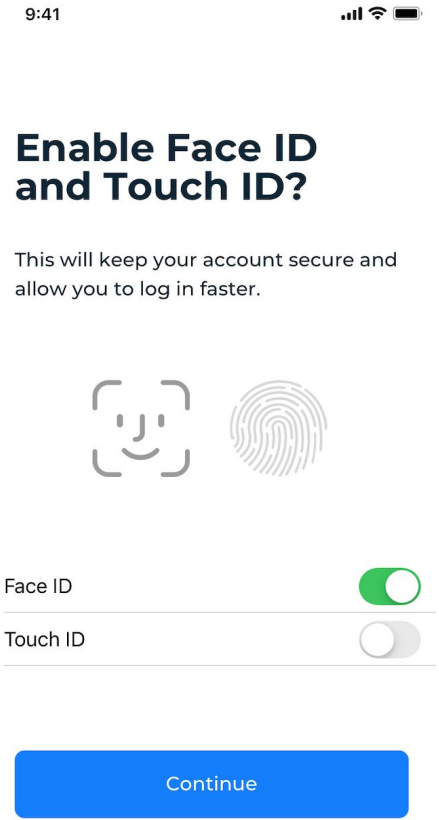


Invitation Workflow in Prefinery - New Password Prompted

Consumer Onboarding Workflow Components

Enrolling a biometric authentication factor

Require a specific user or a user who belongs to a specific group or role to approve a particular stage in the workflow.



Enrolling a biometric authentication factor in a banking application

Authentication

“User authentication is a journey-time process that provides credence in an identity claim by a person already known to an organization.”

Combining Credentials Yields Greater Credence

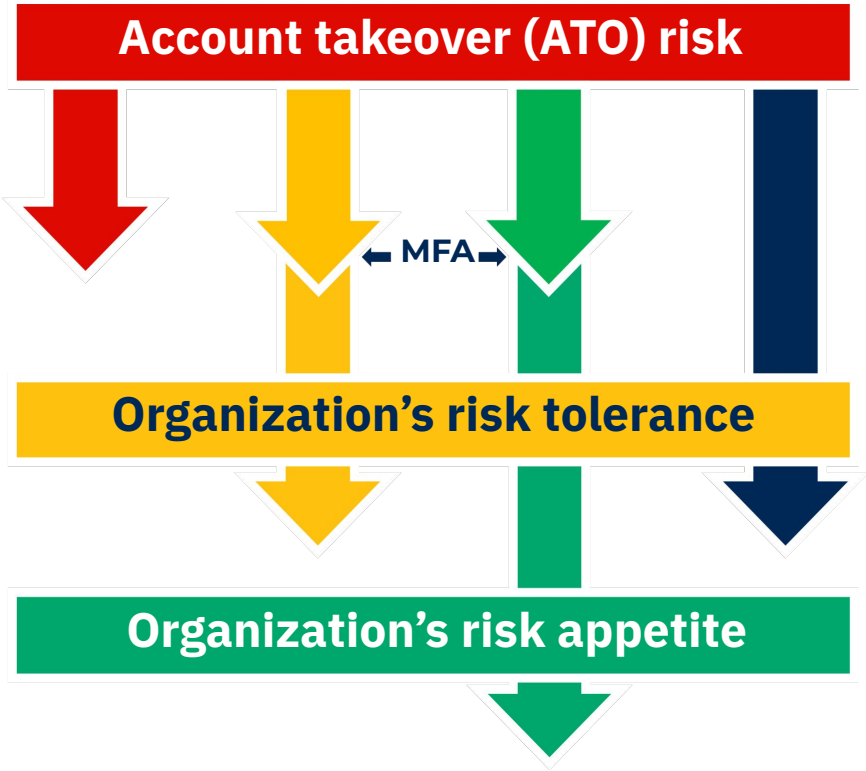
Type 1: Knowledge

Type 2: Tokens (Possession)

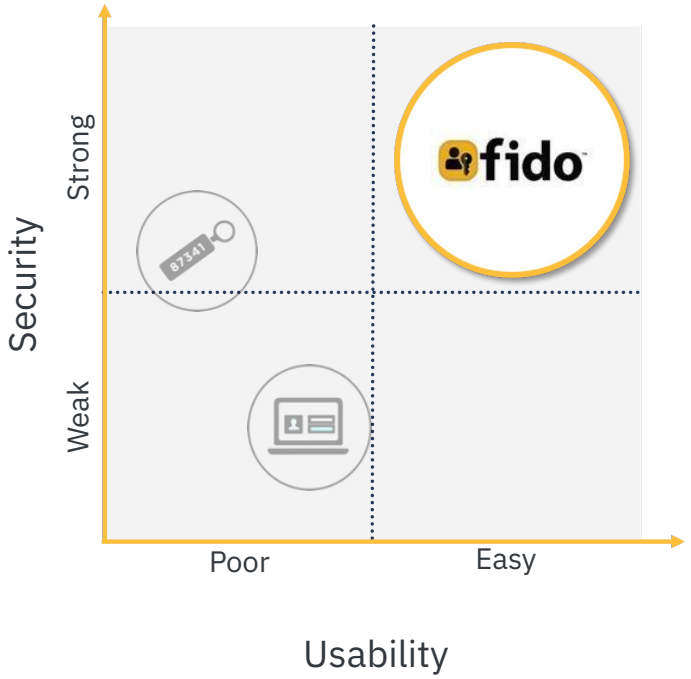
Type 3: Biometrics (Inherence)

Multi-factor authentication (MFA) combines different types

A single factor may be enough if the credential is strong enough



FIDO: Simpler and Stronger



=

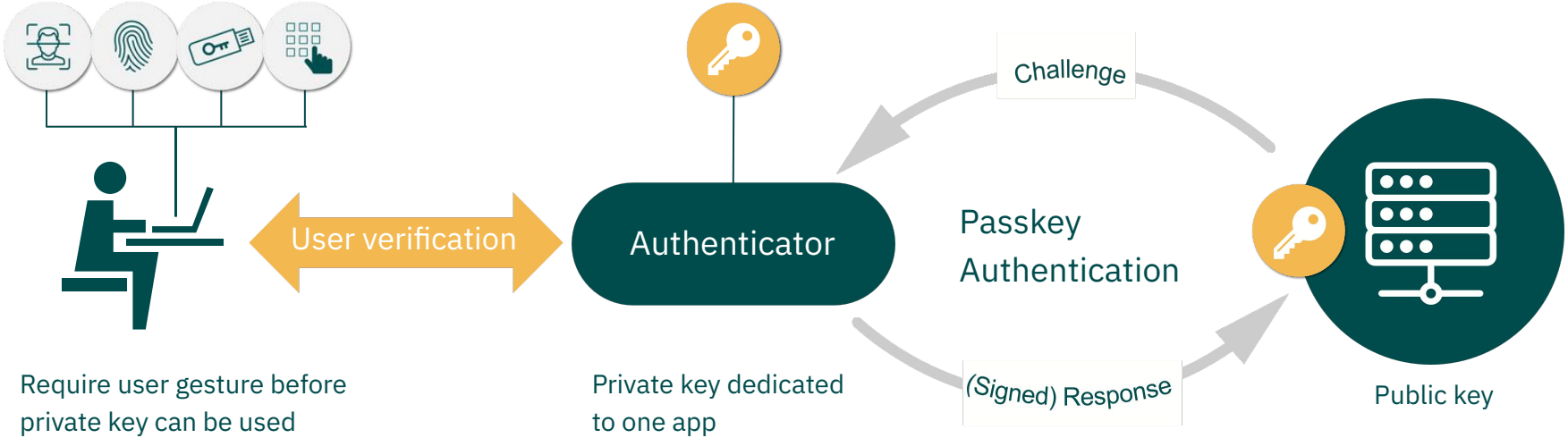
Open standards for simpler, stronger authentication using public key cryptography

– Single Gesture –

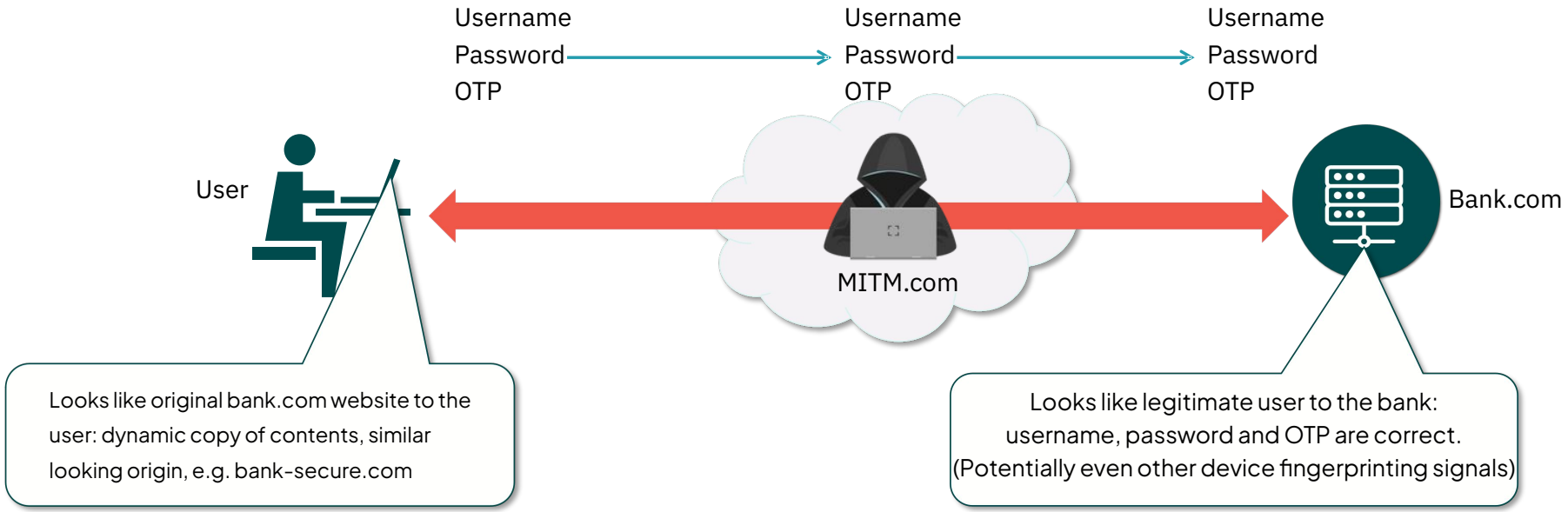
– Possession-based –

– Phishing-resistant –

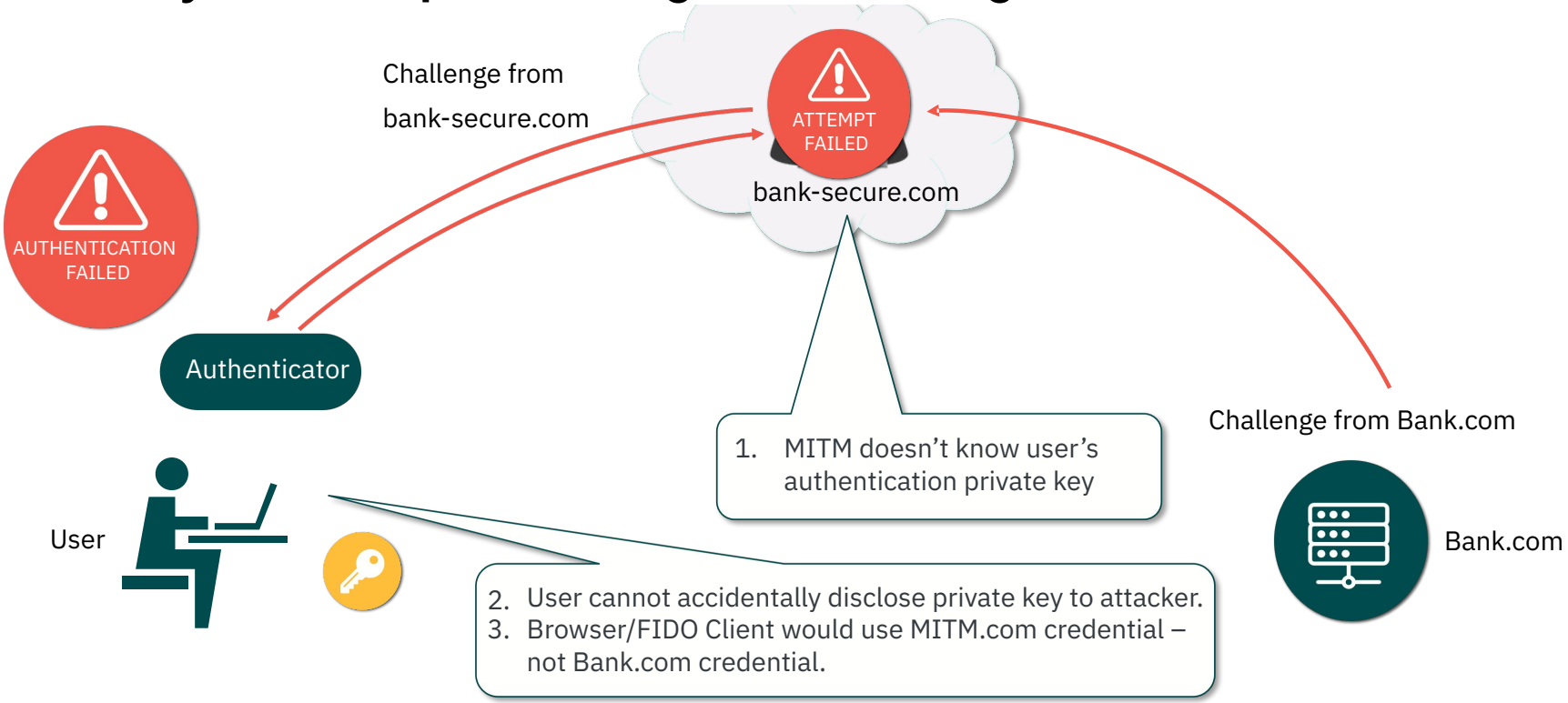
Passkey Authentication: How It Works?



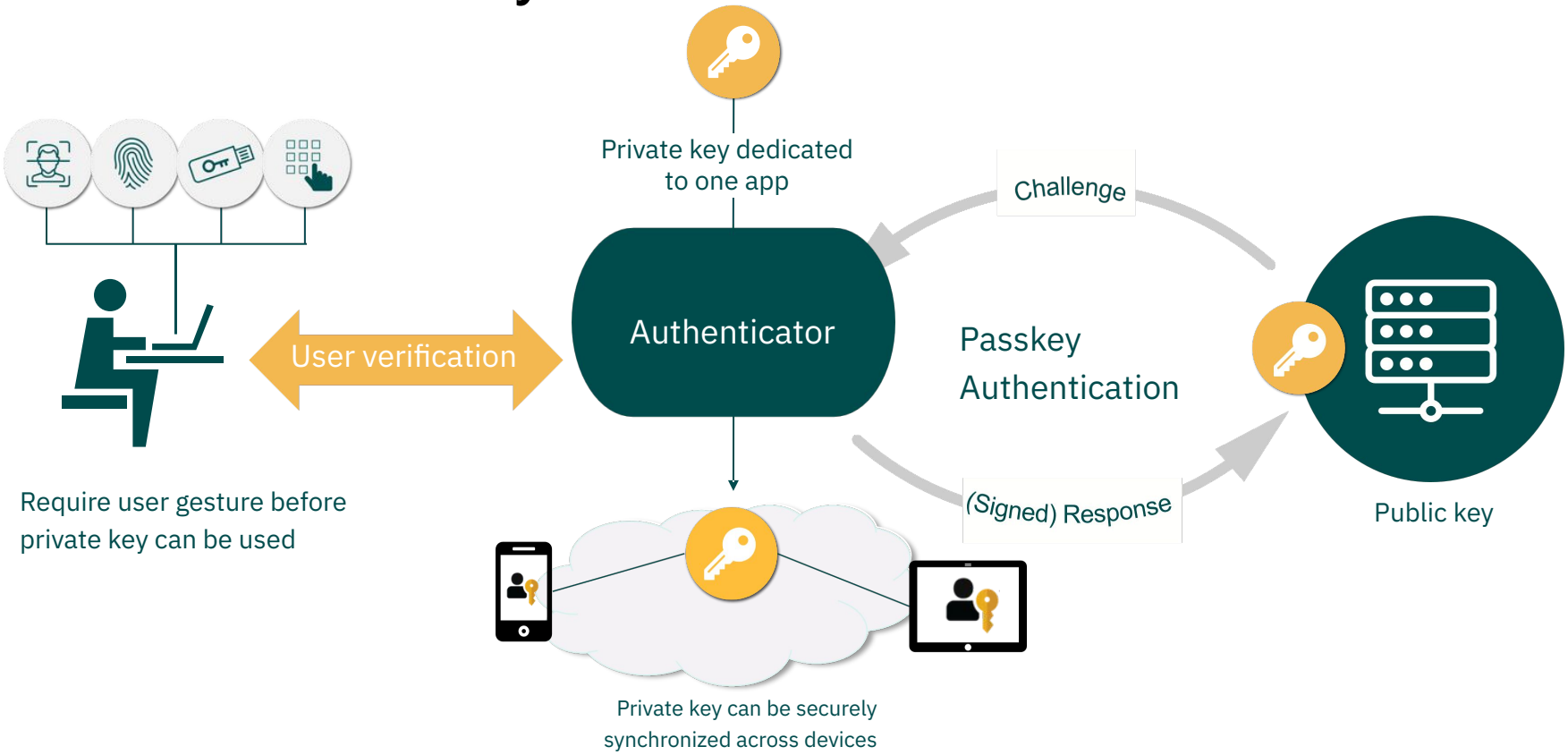
Passwords and Legacy MFA: Vulnerable to Man-in-the-Middle attacks (aka phishing)



Passkeys: How it protects against Phishing?



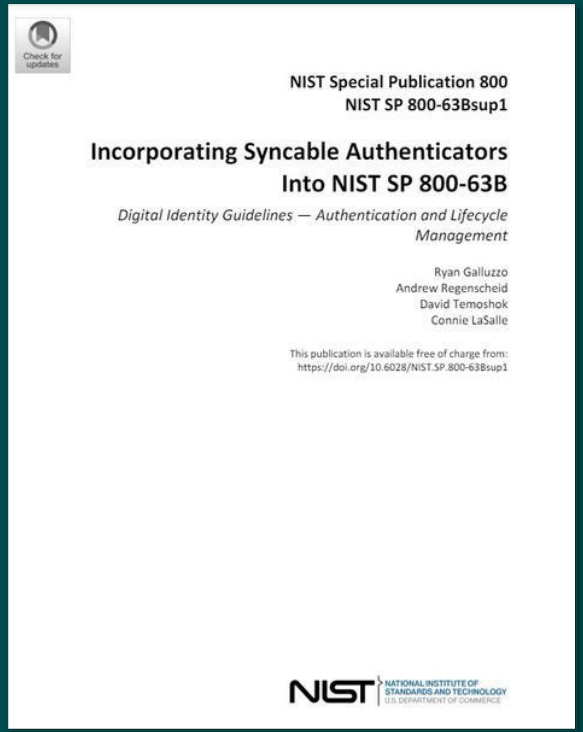
Multi-device Passkeys



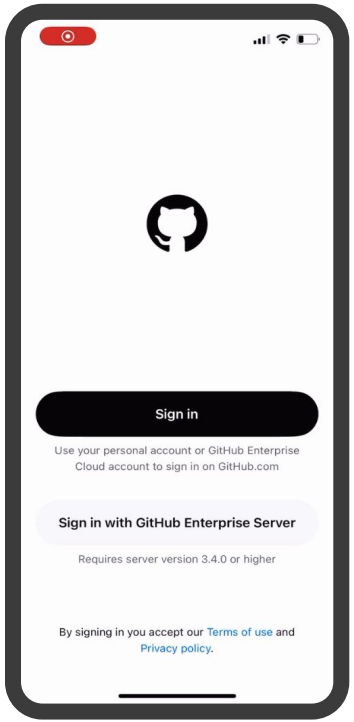
A closer look at NIST support of passkeys

NIST supplement:

- Recognizes synced authenticators as AAL2
- Device-bound authenticators remain AAL3



Redirect-based Sign-In Experience



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.

App-Native Sign-In Experience

REDIRECT-BASED

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

Results in a potentially disjointed user experience



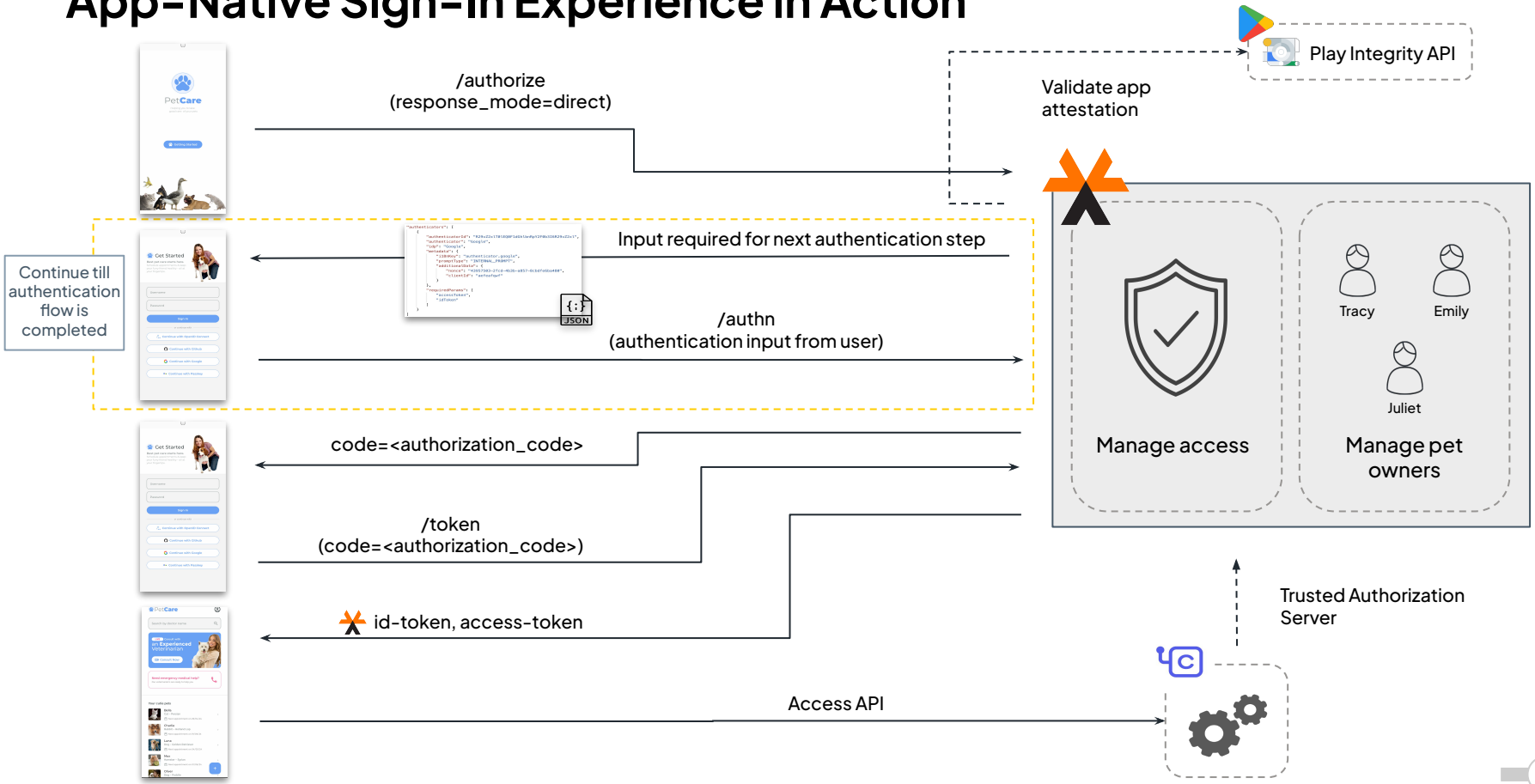
NATIVE



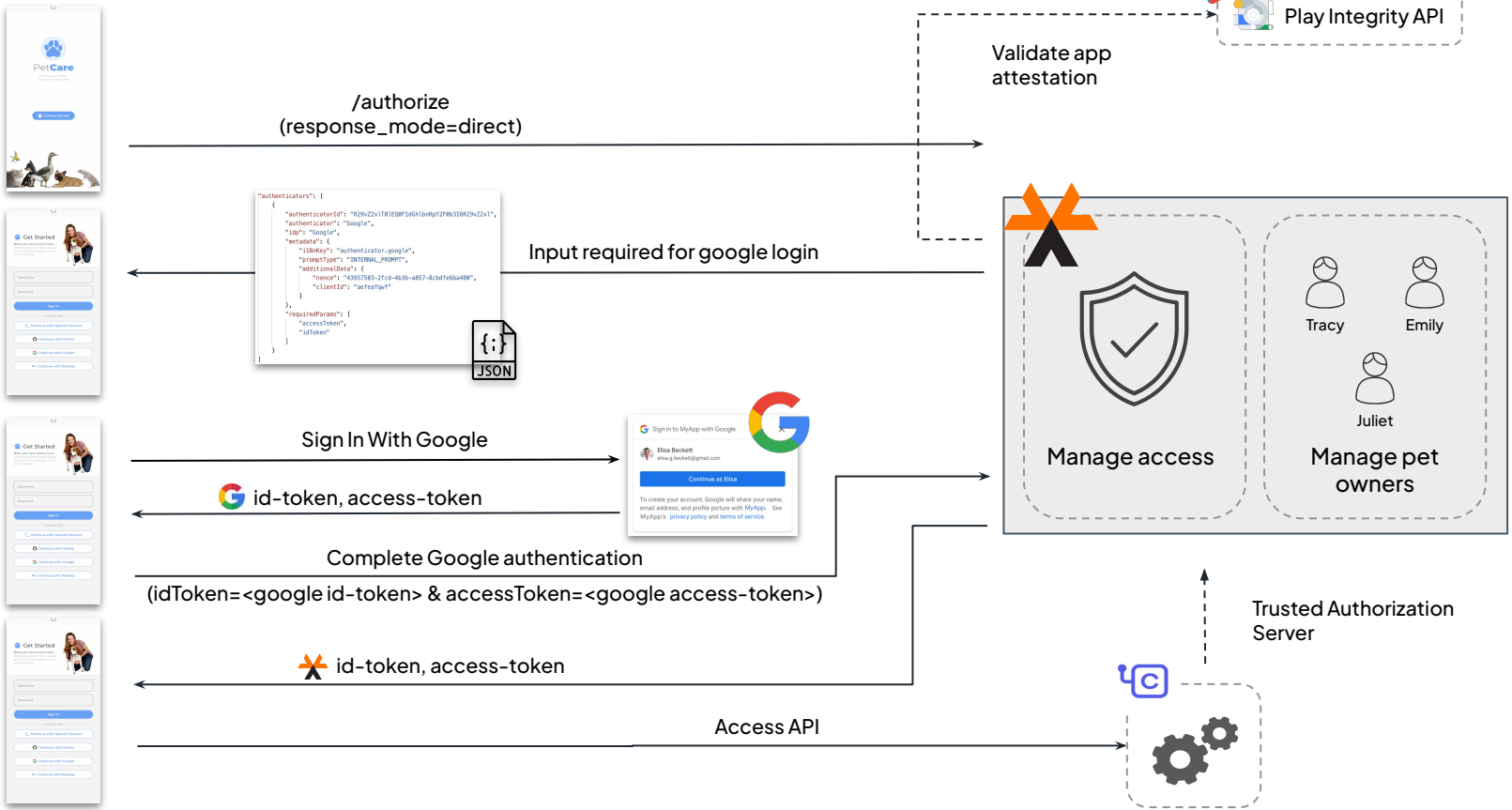
User never leaves the native application while logging in

Enables a more seamless, user-friendly authentication flow

App-Native Sign-In Experience in Action

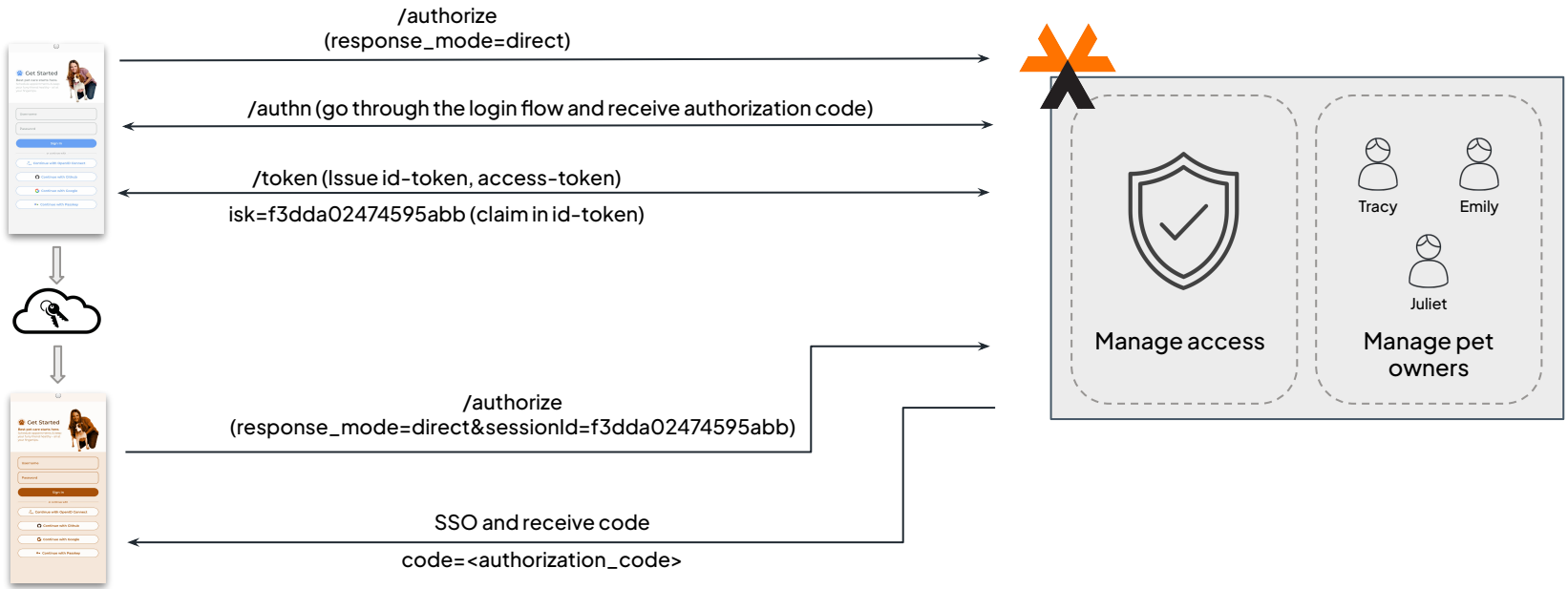


App-Native Sign-In Experience with Google



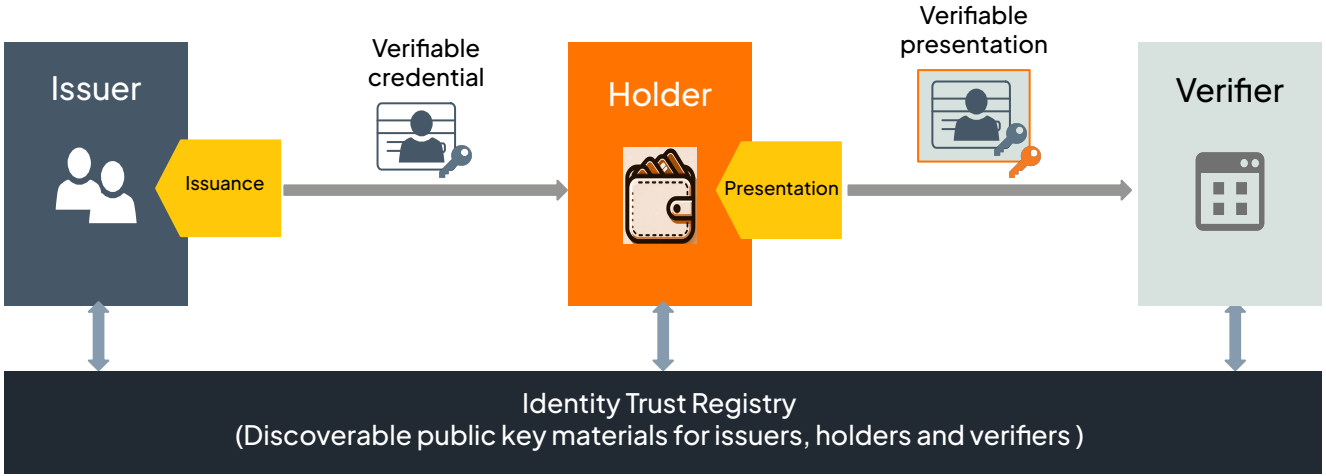
SSO with App-Native Sign-In Experiences

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



Decentralized Identity and Verifiable Credentials

Zero-knowledge Proofs



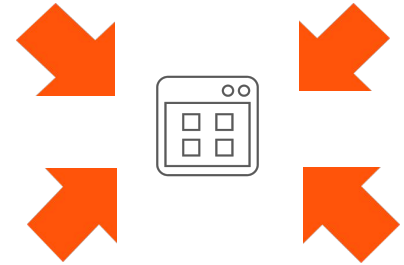
Recognition and Risk Signals

Situations signals

- Credential block lists
- Device identity and profiling
- Network identity or IP geolocation
- Device security posture

Behavioural signals

- Passive behavioral biometrics
- Bot mitigation
- Event intelligence (access and session behavior)



Credential-based outcomes

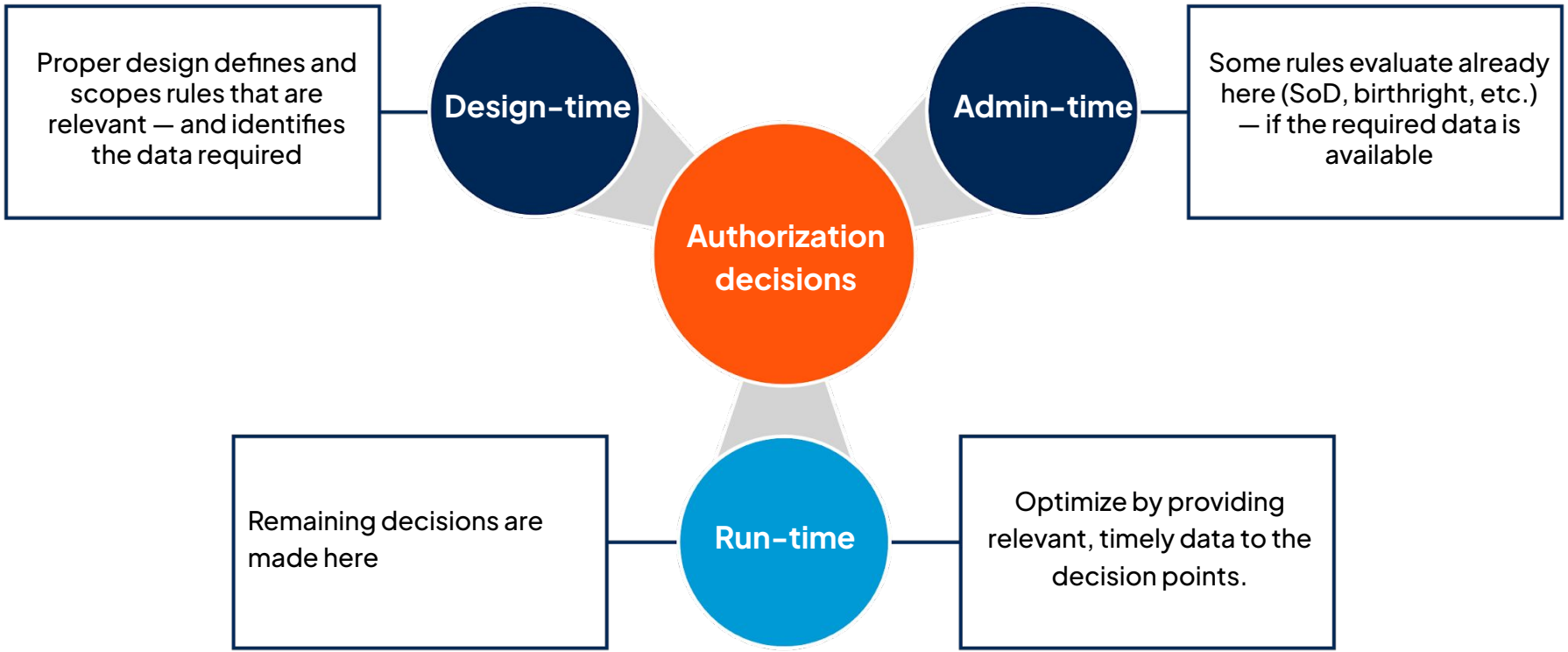
- Face
- Fingerprint
- Voice
- Iris
- Hand
- Gait

Shared signals (e.g. CAEP)

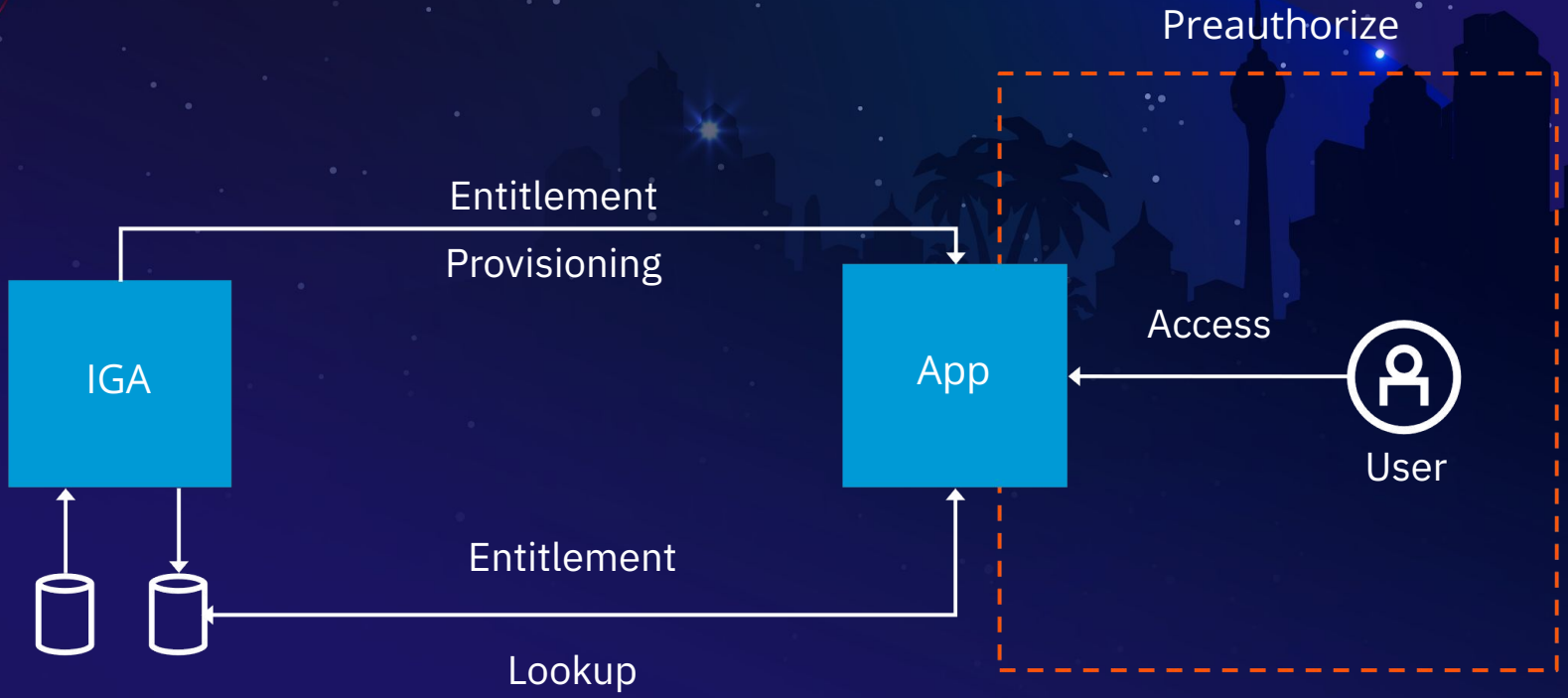
- Session revoked
- Token claims change
- Credential change
- Assurance level change
- Device compliance change

Authorization

Aspects of Authorization

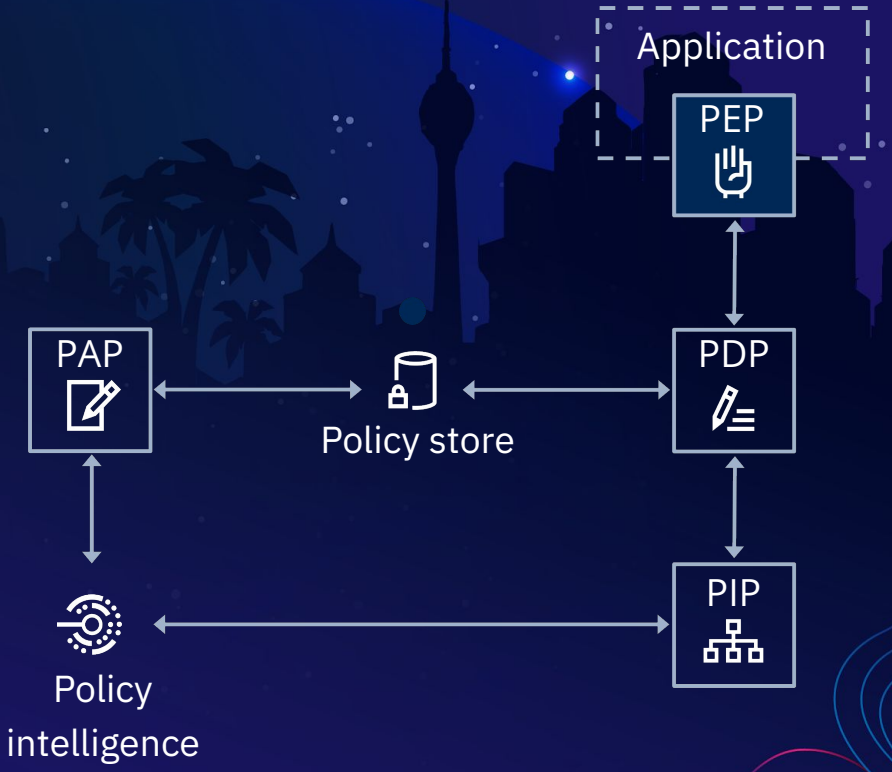


Admin –time Authorization

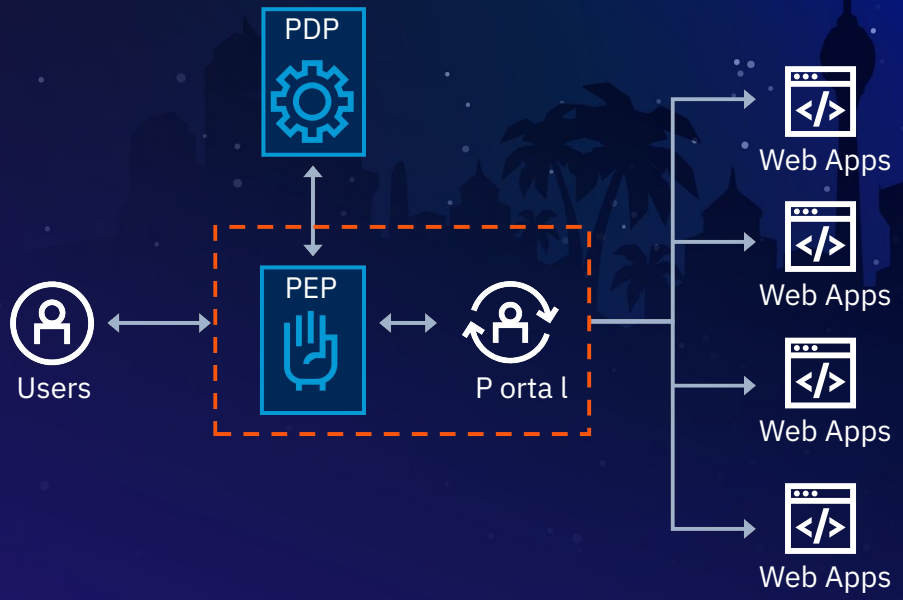


Run-time Authorization Components

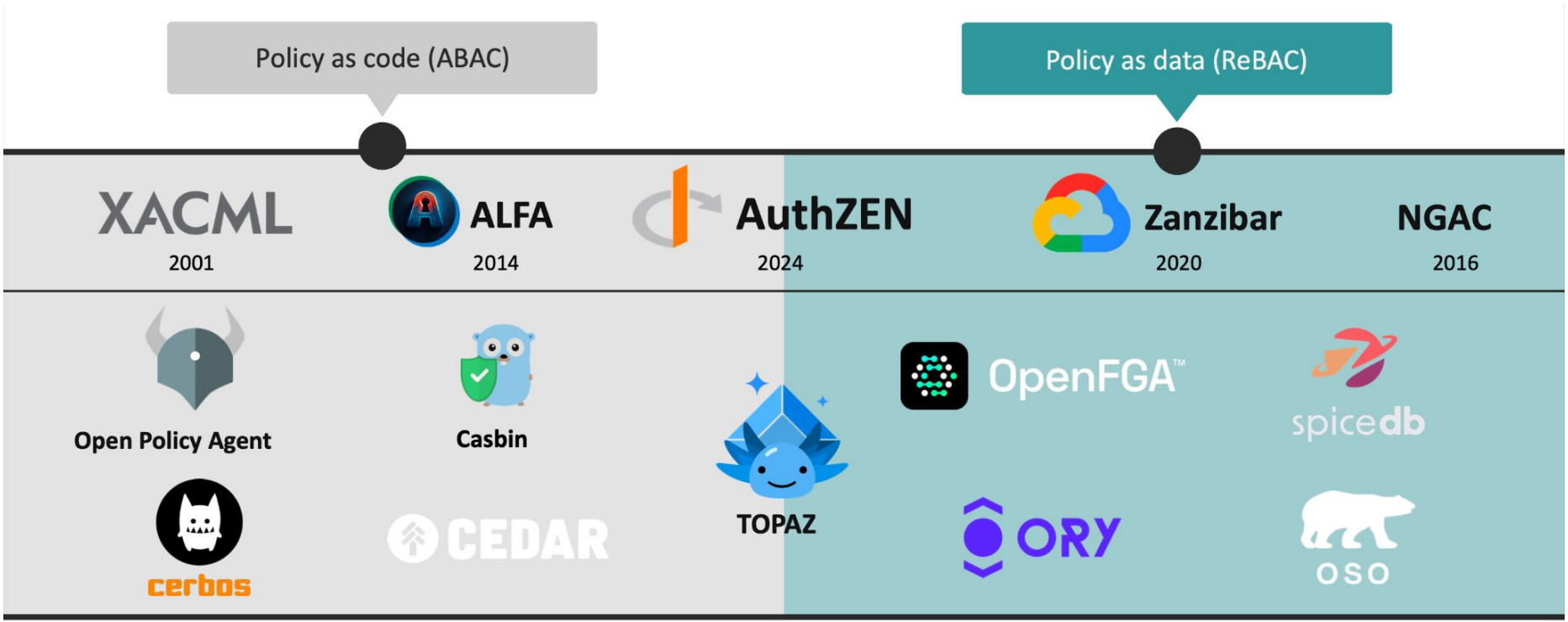
- PEP: Policy enforcement point
- PDP: Policy decision point
- PIP: Policy information point
- PAP: Policy administration point
- Policy store
- Policy intelligence



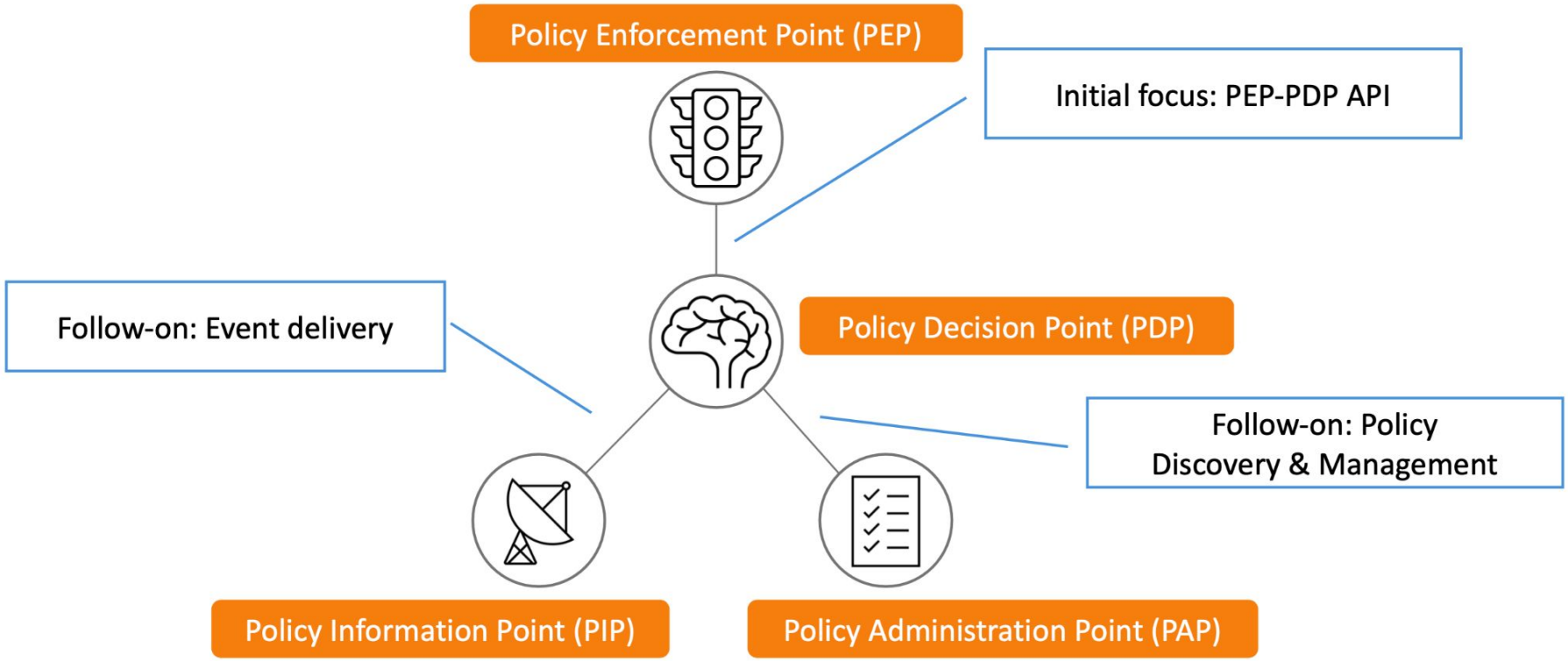
Portal Access



Modern Authorization



The AuthZEN Charter



Access Delegation



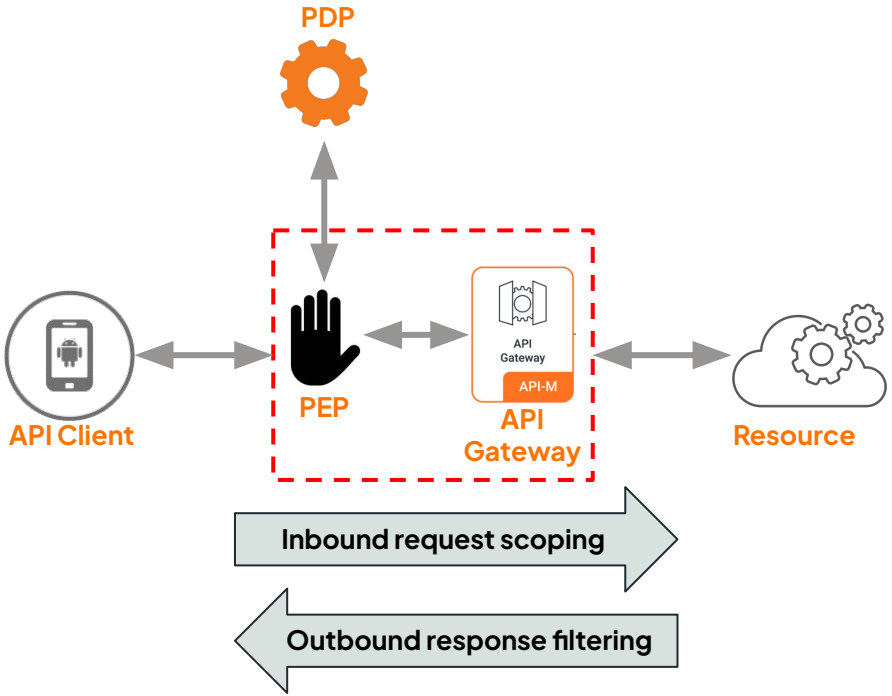
Zero Trust Security Architecture (ZTSA)

Zero trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk/trust levels based on identity and context supported by security infrastructure that adapts to risk-optimize the organization's security posture.

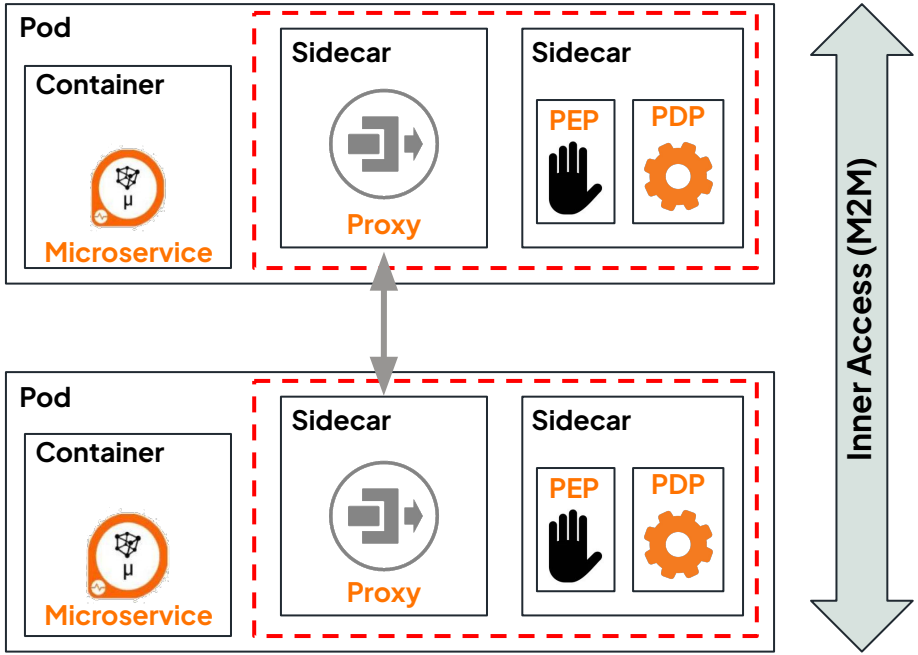
.

Source: https://www.linkedin.com/pulse/zero-trust-modern-security-architecture-lahiru-livera/

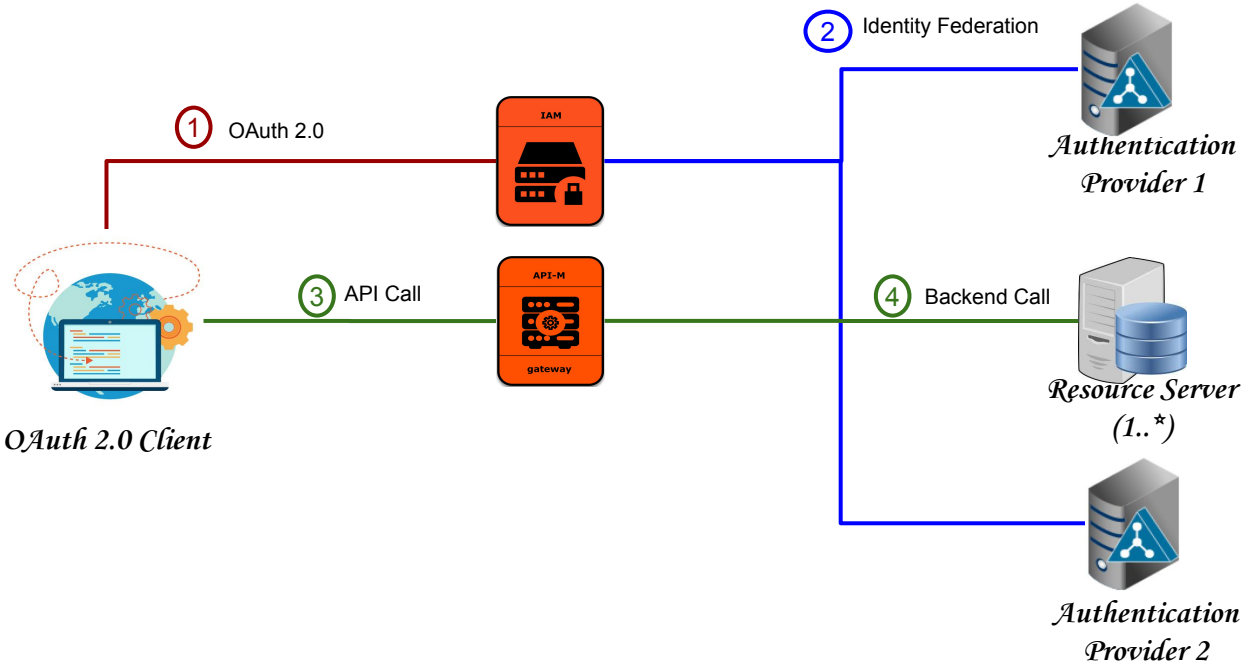
API Gateway Architecture



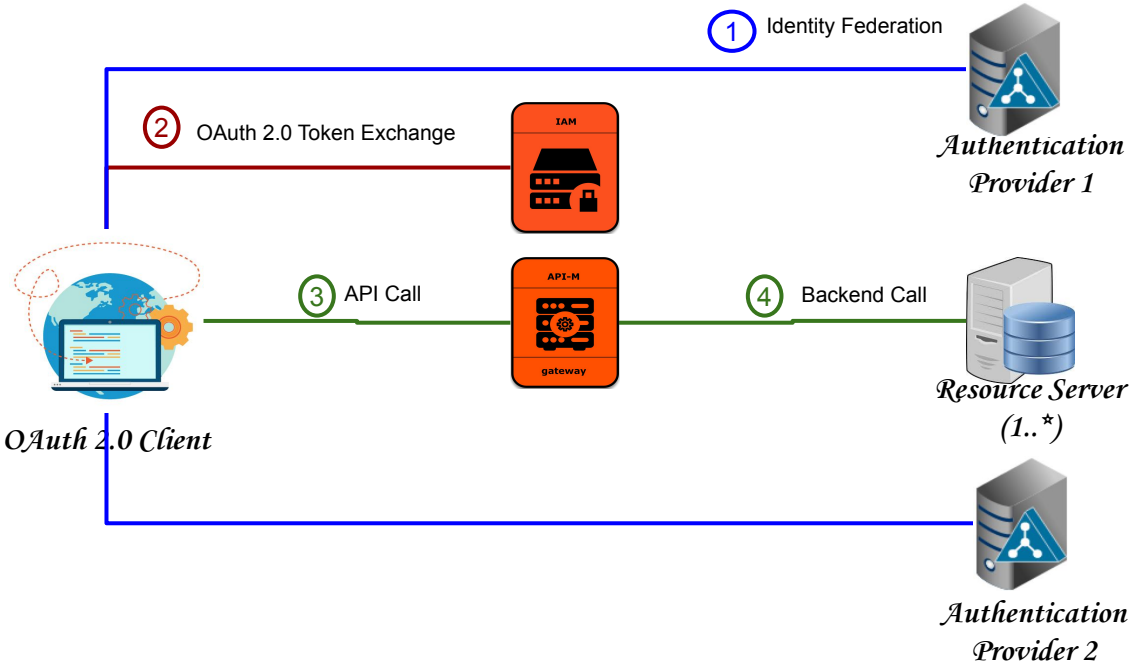
Service Mesh Architecture



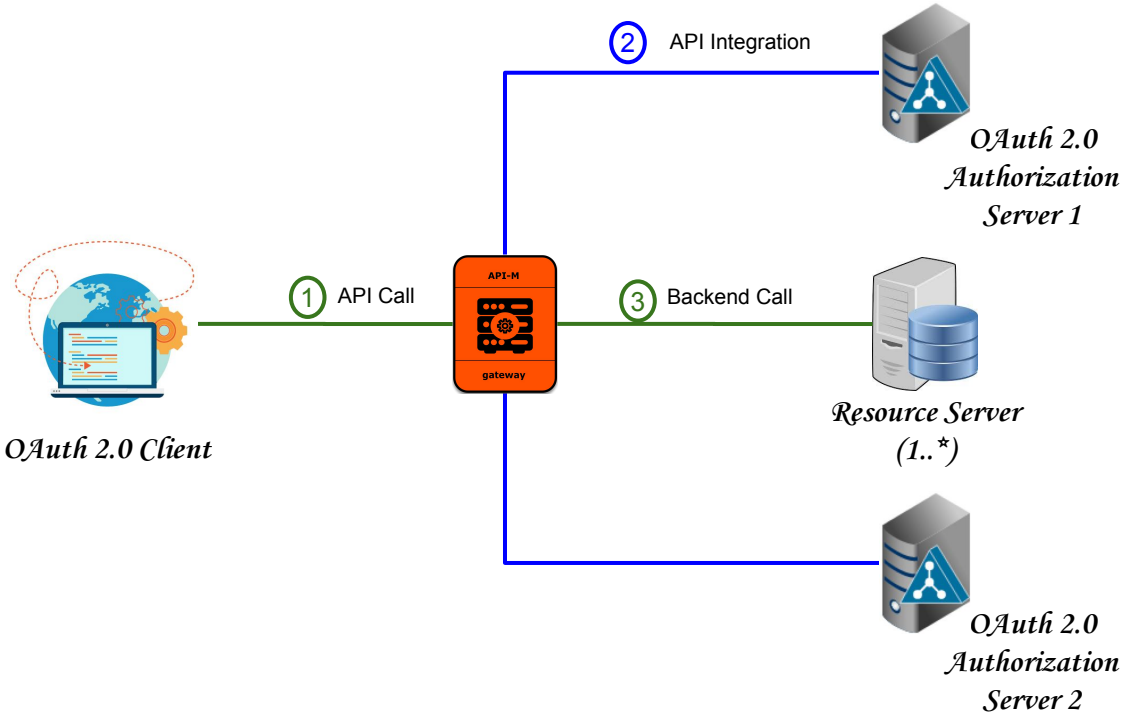
Distributed Authentication Providers – Front-channel Federation



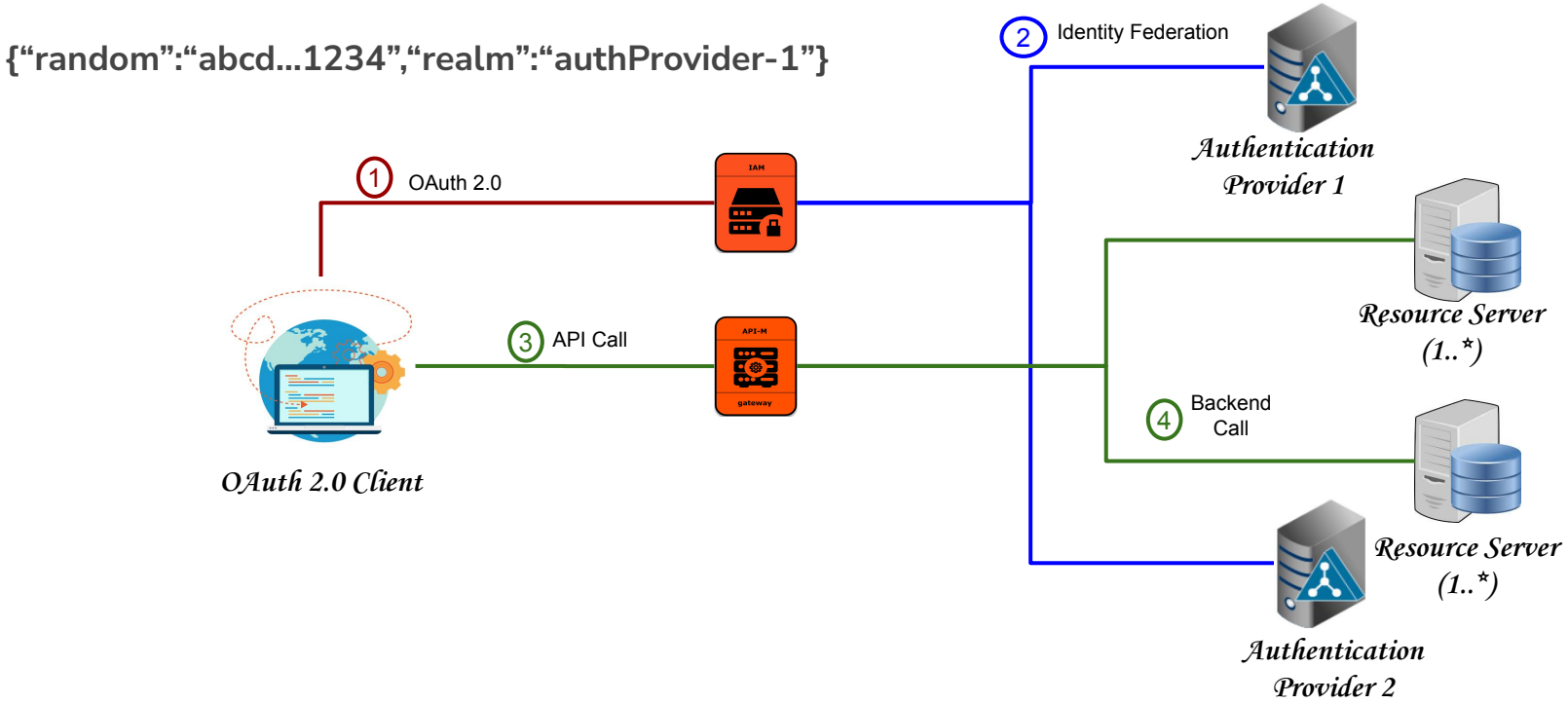
Distributed Authentication Providers – Back-channel Federation



Distributed Authorization Servers

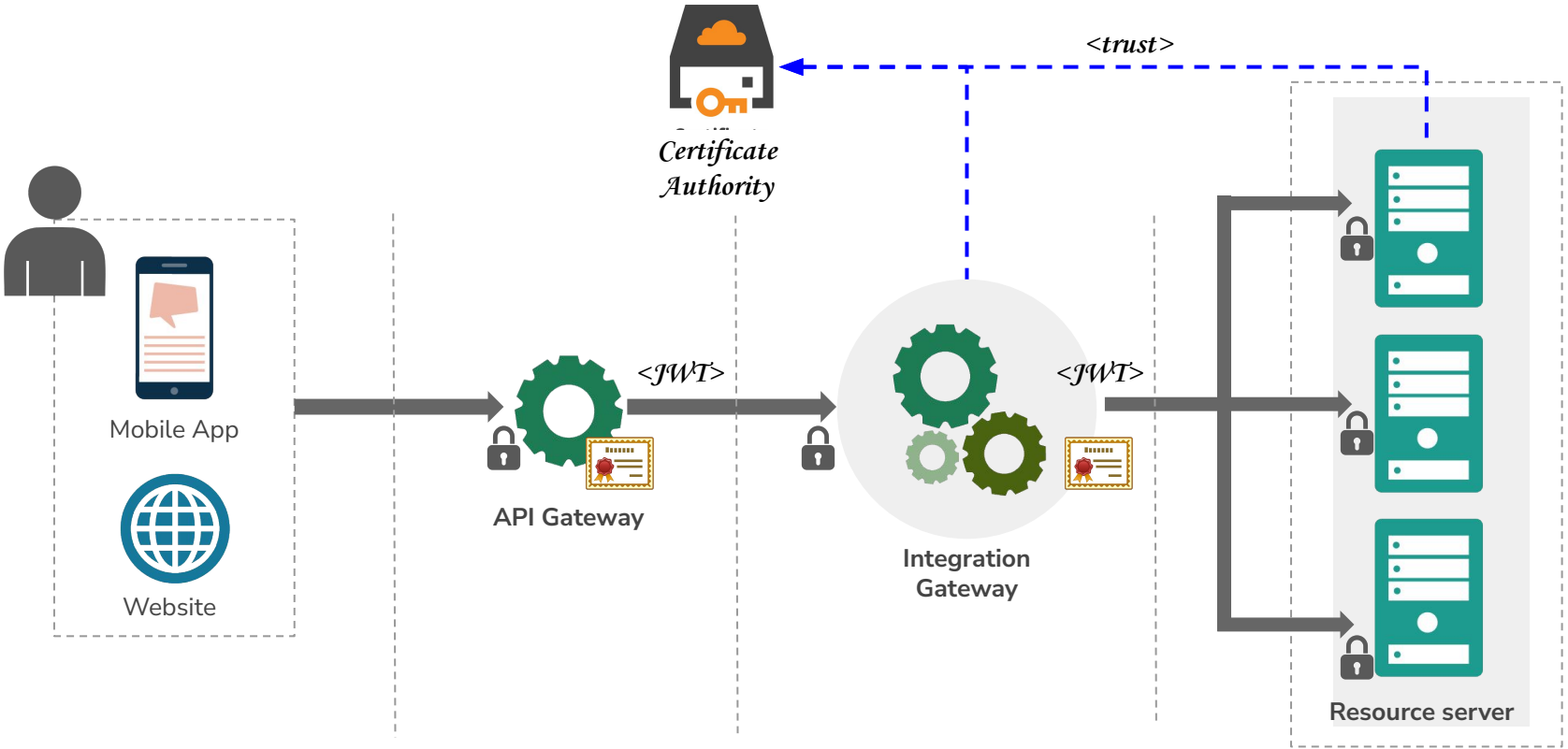


Distributed Authentication + Resource Servers



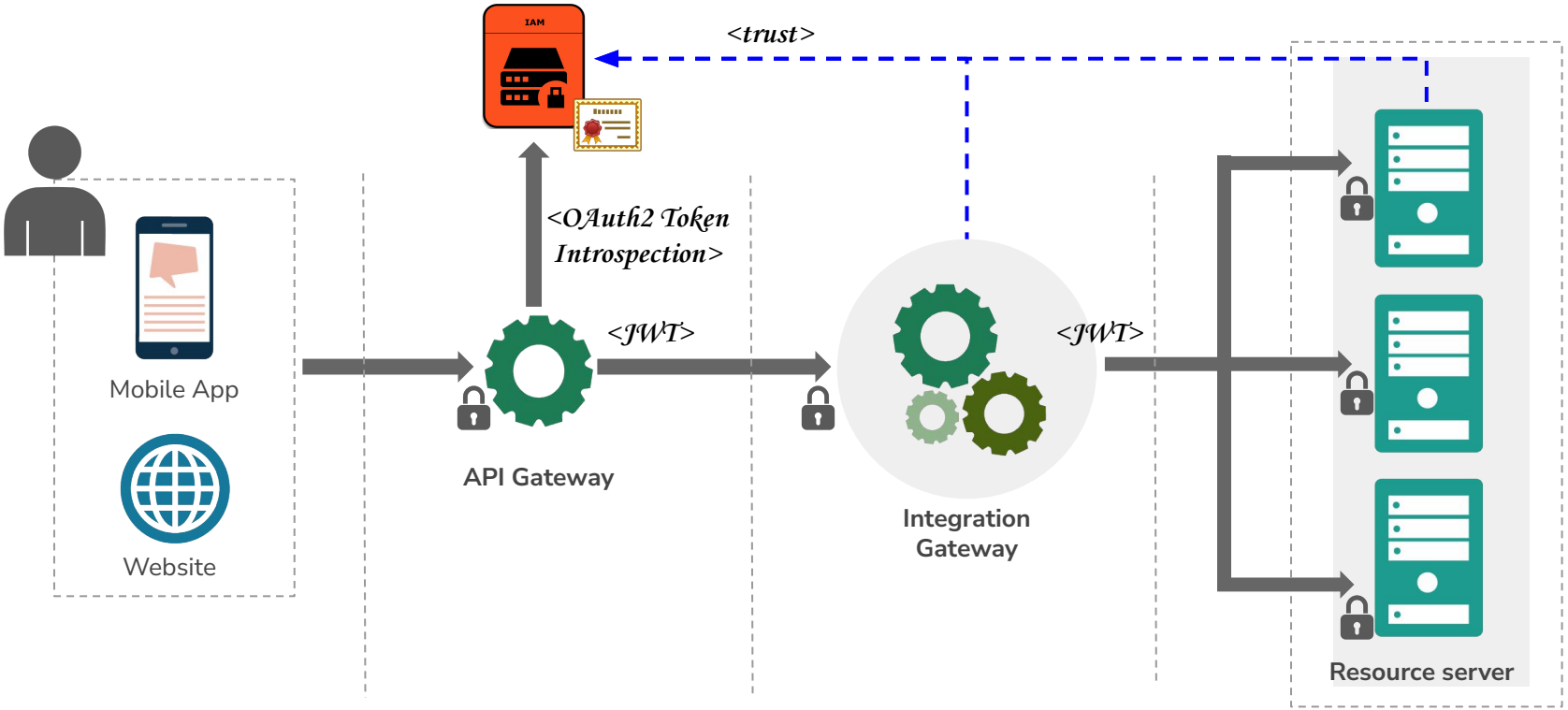
Trusted Subsystem

Trusted subsystem generated identity token

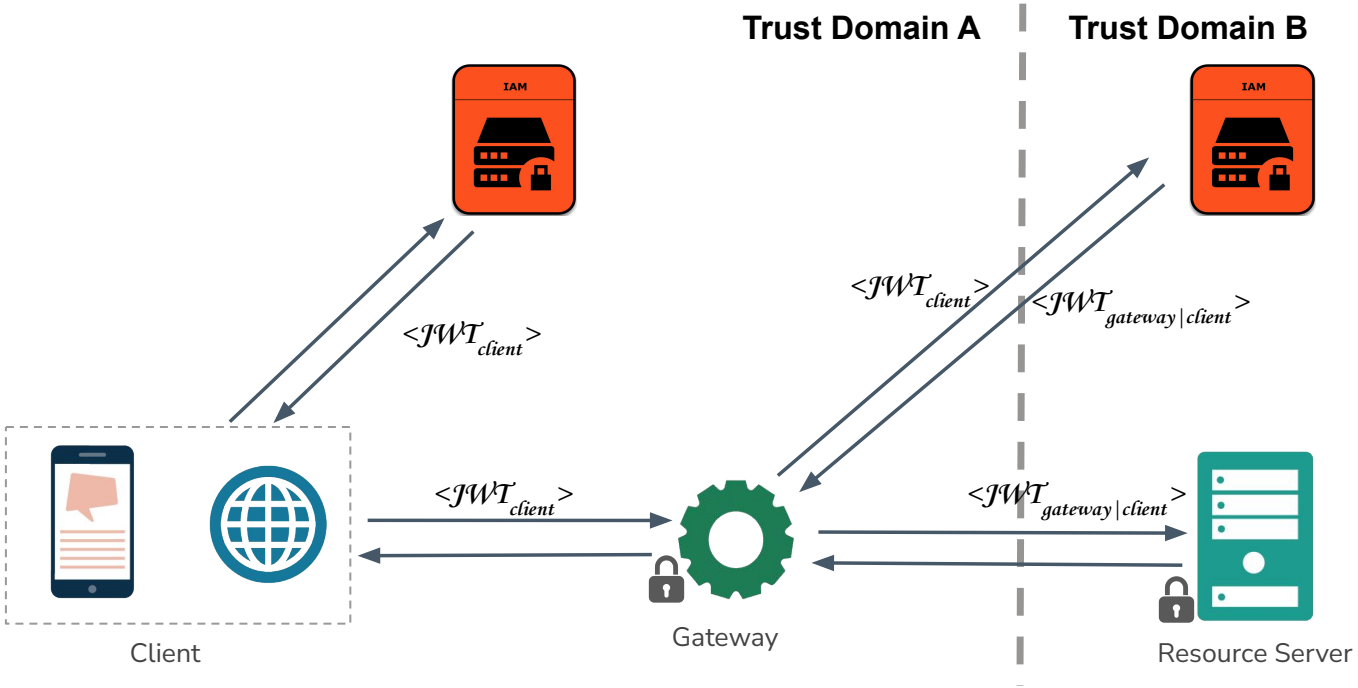


Trusted Subsystem

Third-party generated identity token

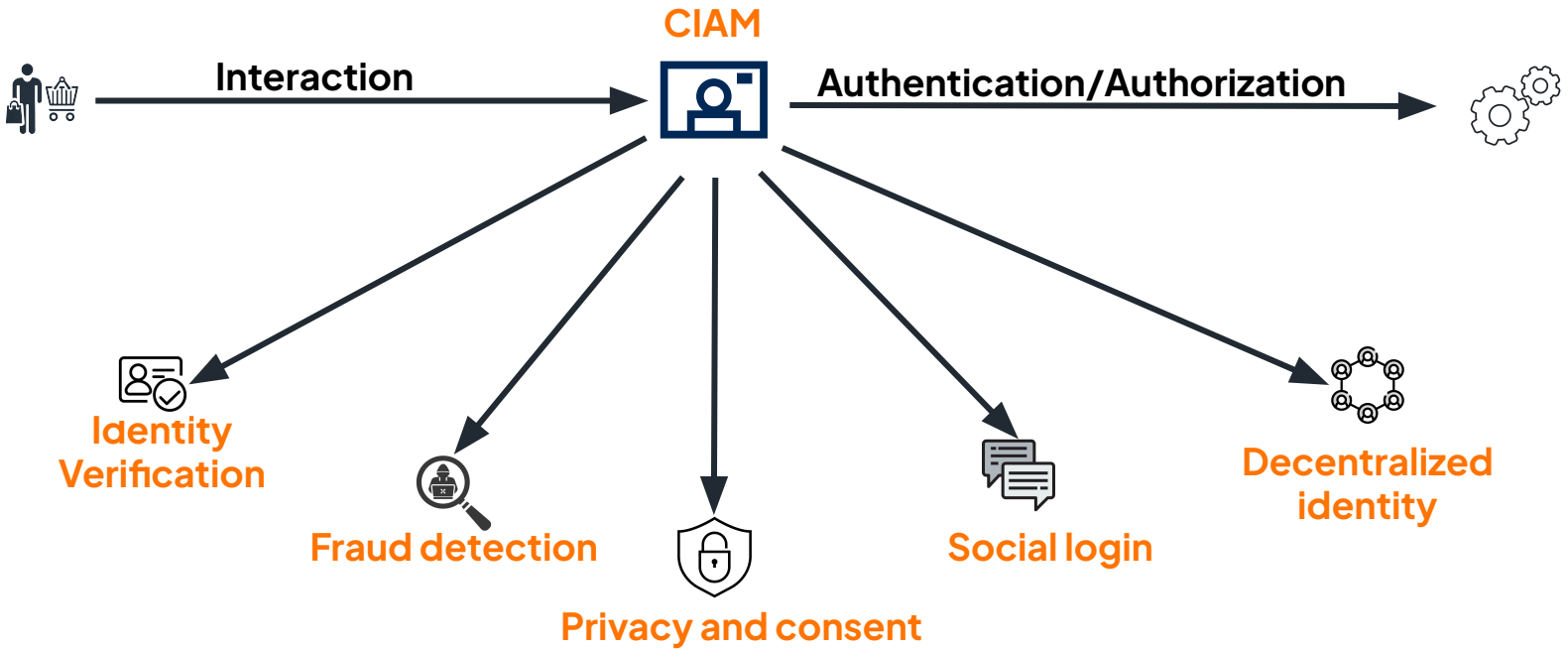


Token Exchange (On-Behalf-Of)



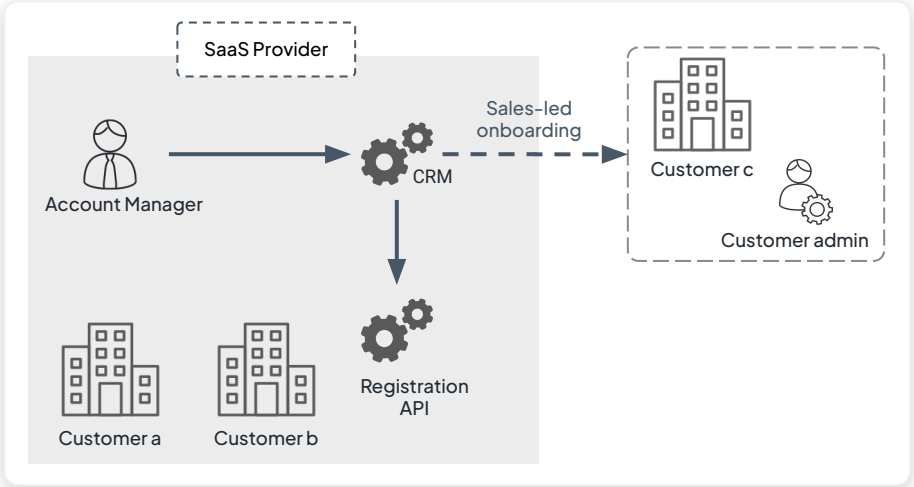
CIAM Ecosystem

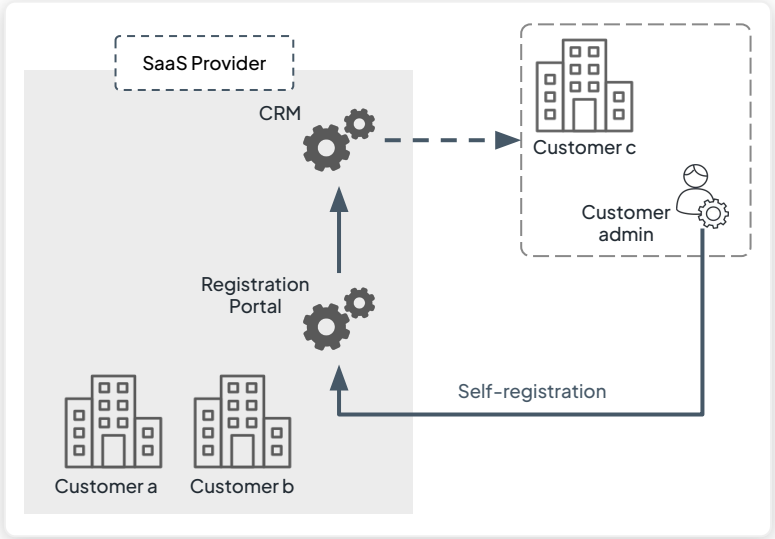
Identity Orchestration via API and Events

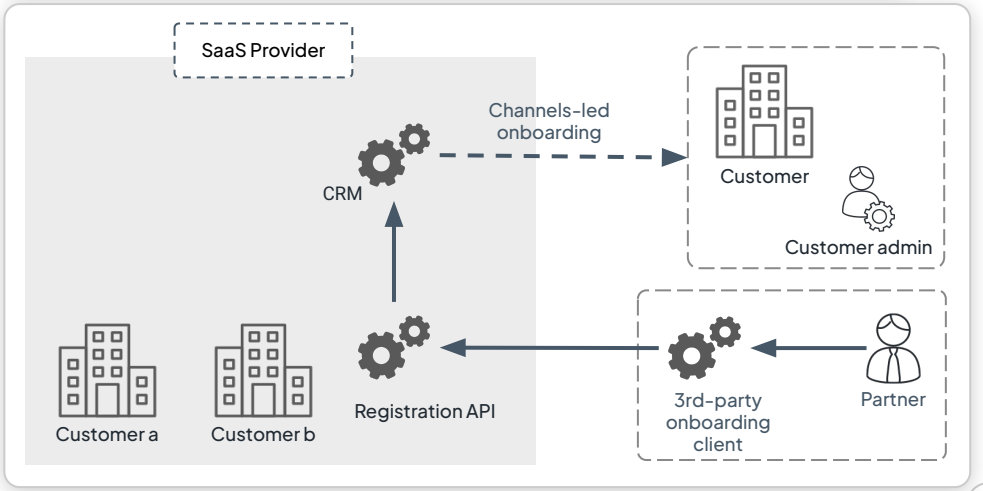


Integrations

Transforming internal processes by integrating with systems such as CRM, subscription services, marketing automation, and CDPs

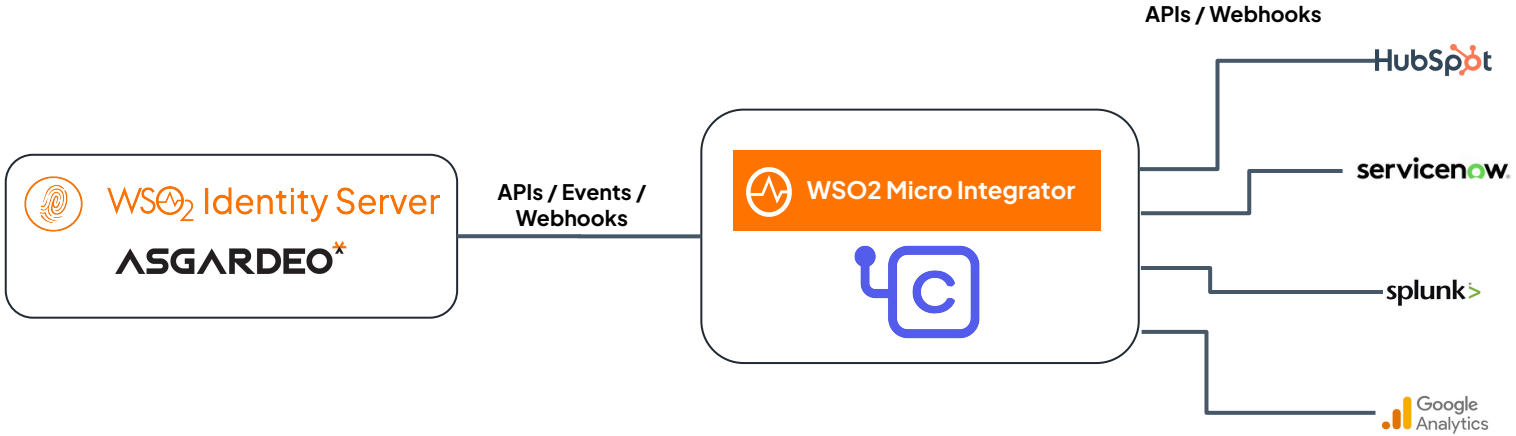




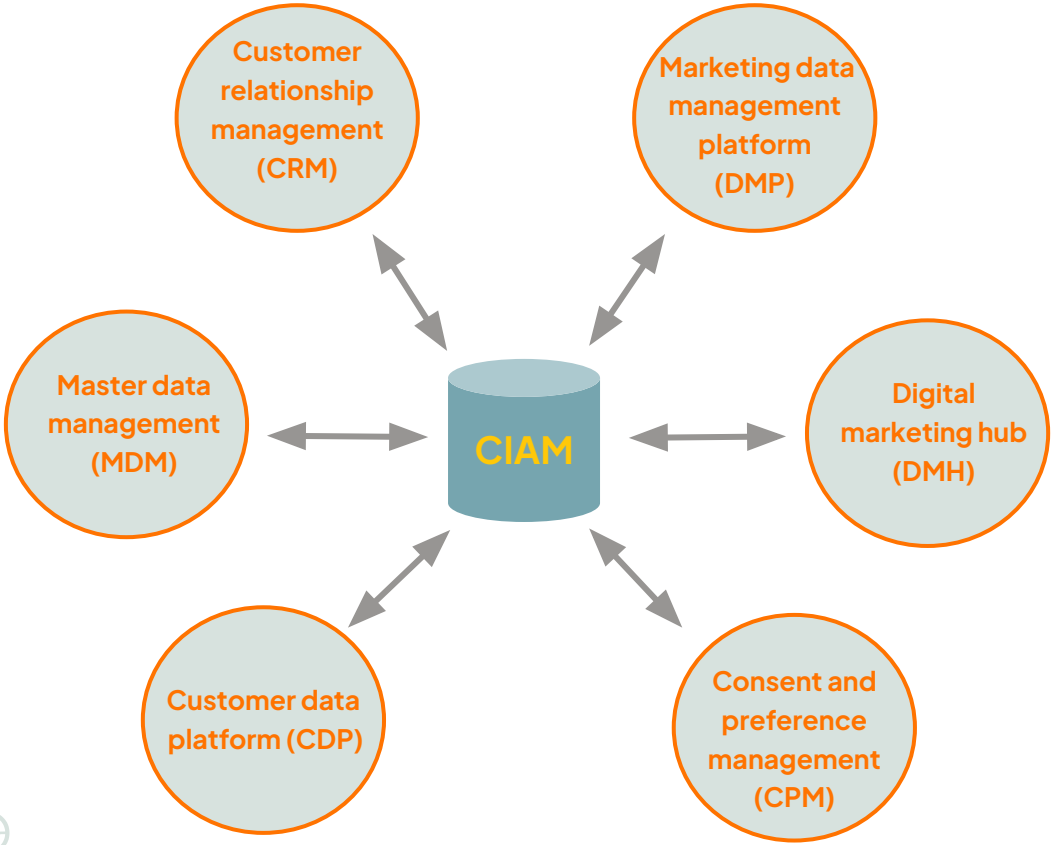


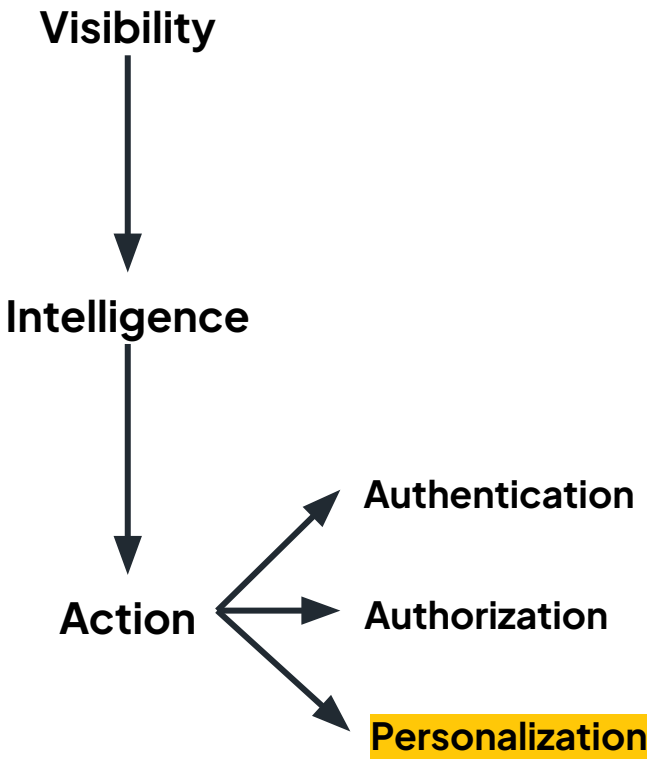
Runtime extensibility

Built-in extension architecture that supports runtime extensibility without having to recompile or redeploy software. Serverless architectures in the cloud make it even more easier for developers to write and deploy extensions

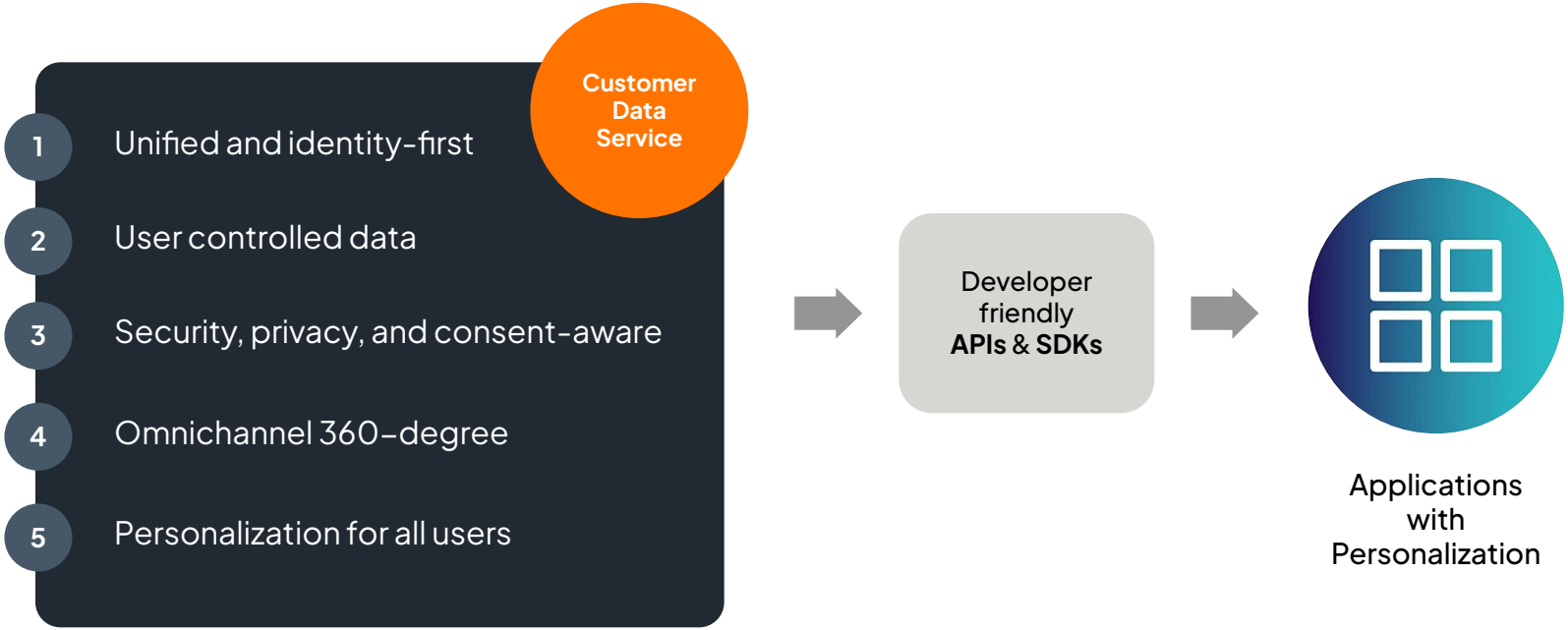


CIAM is Connected!



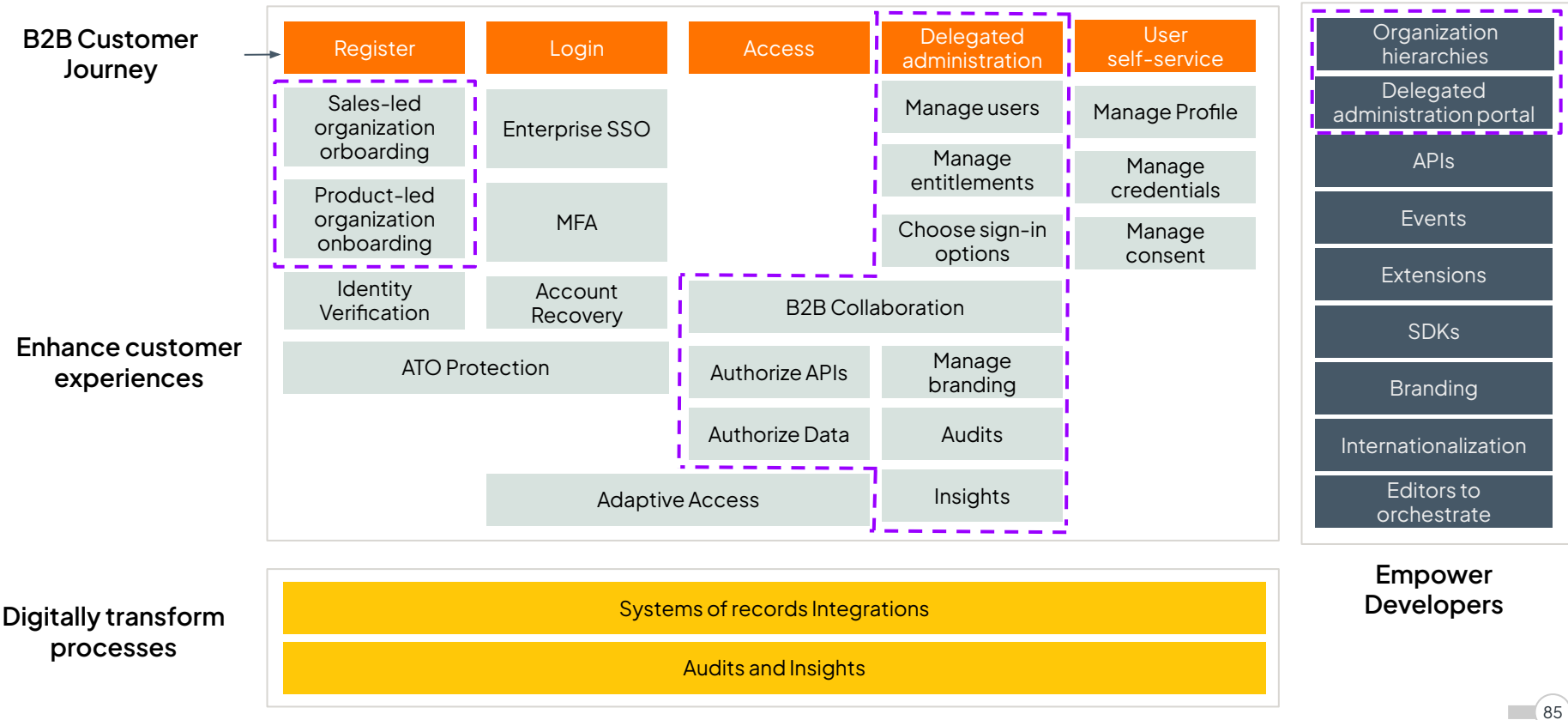


Customer Data Service

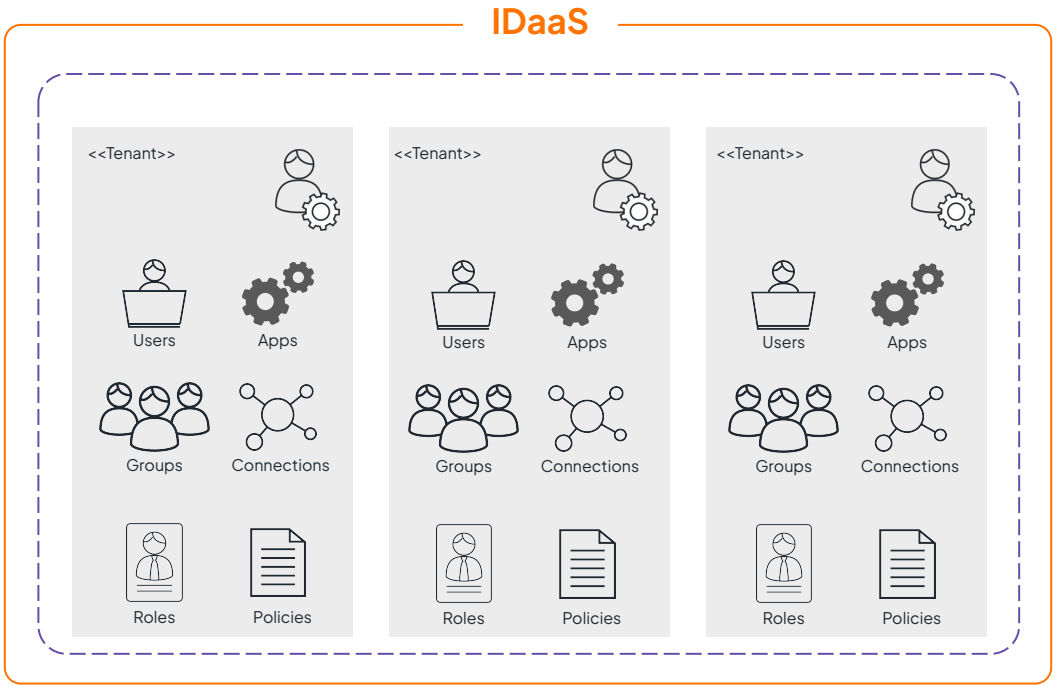


IAM for Business-to-Business (B2B) Applications

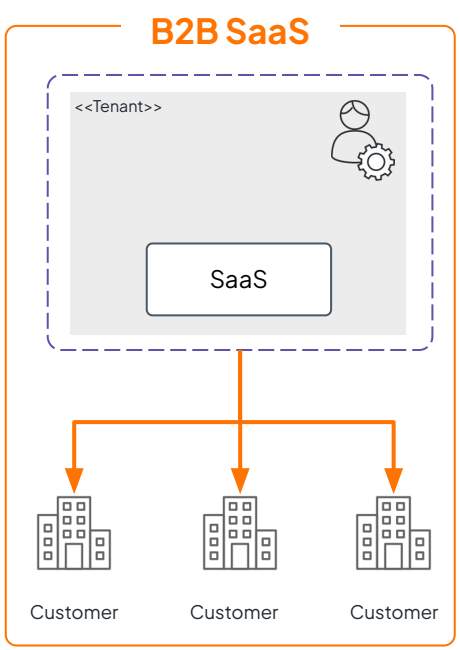
Critical capabilities for effective CIAM in B2B SaaS apps

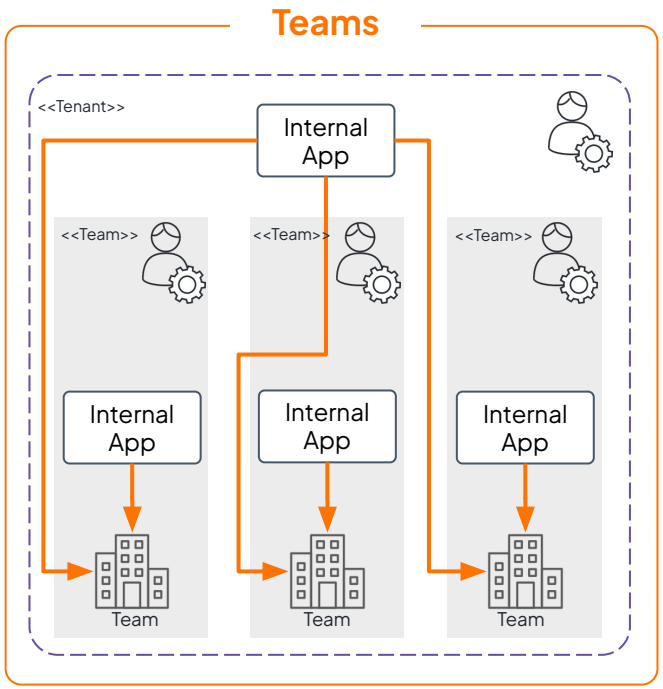


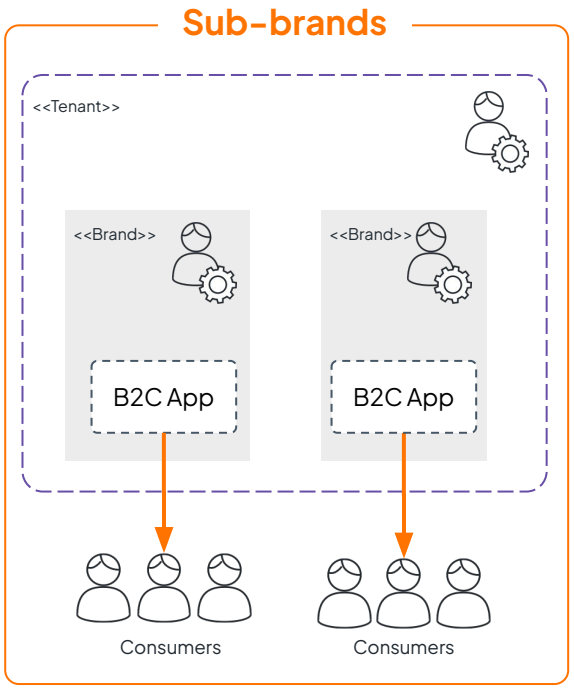
Organizations



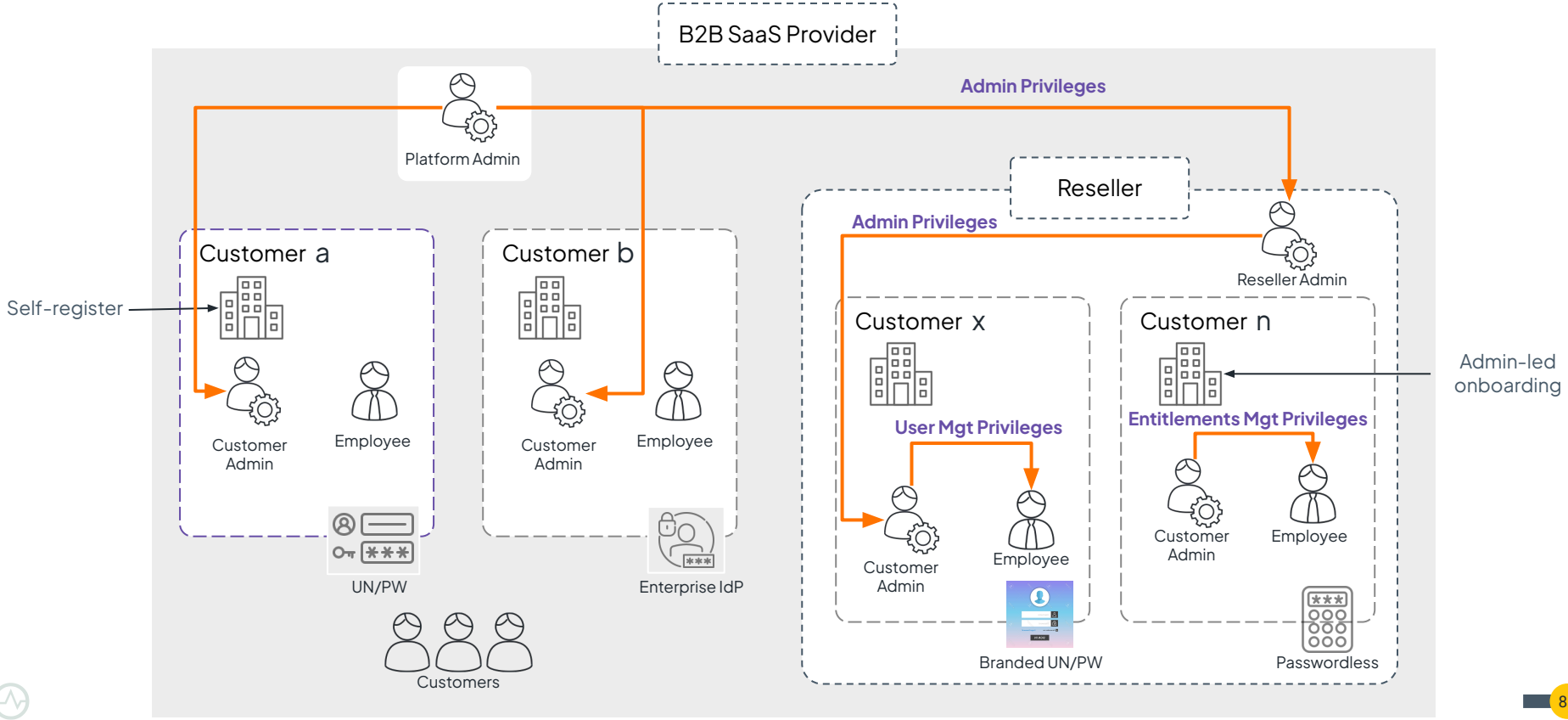
Sub-organization models



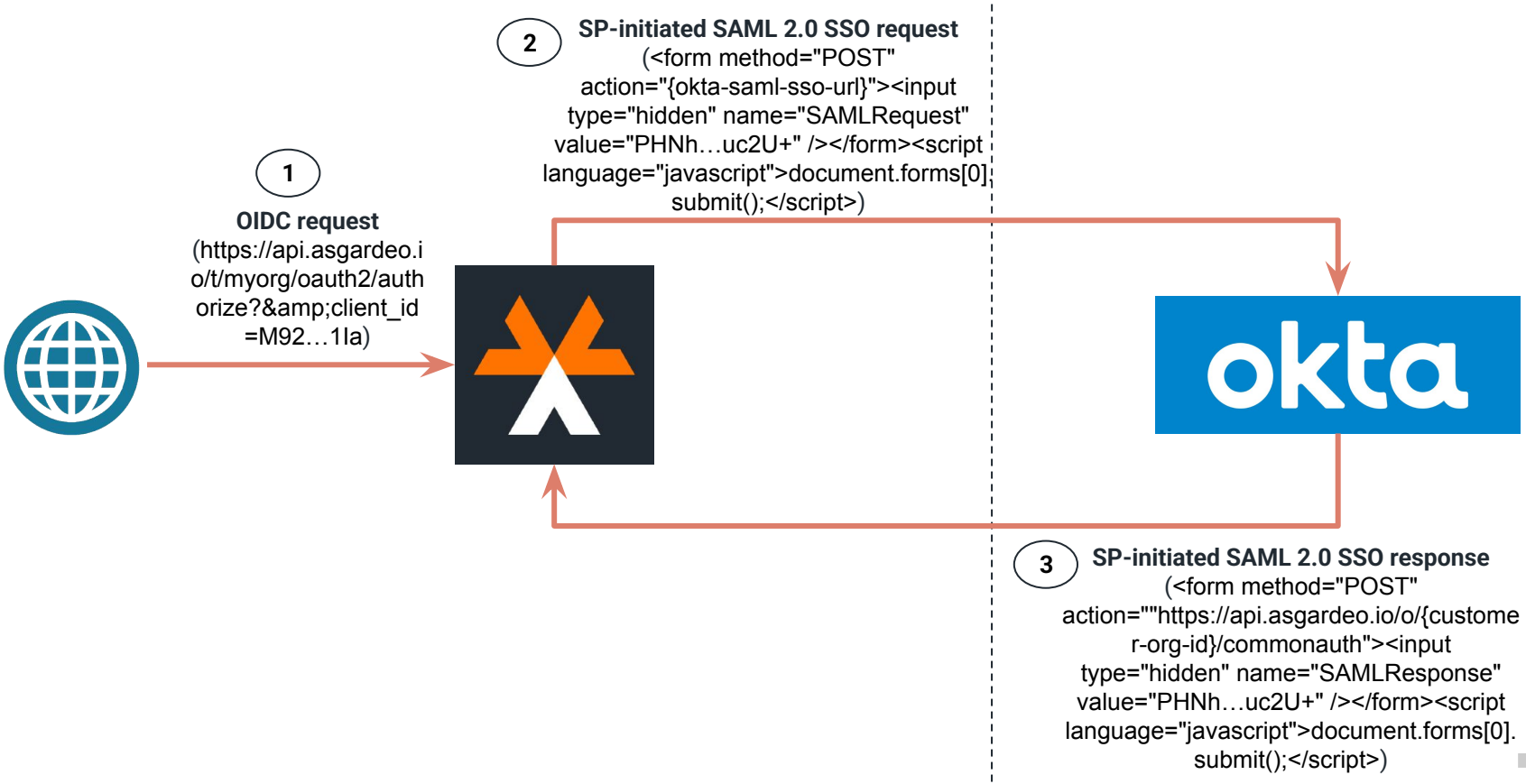




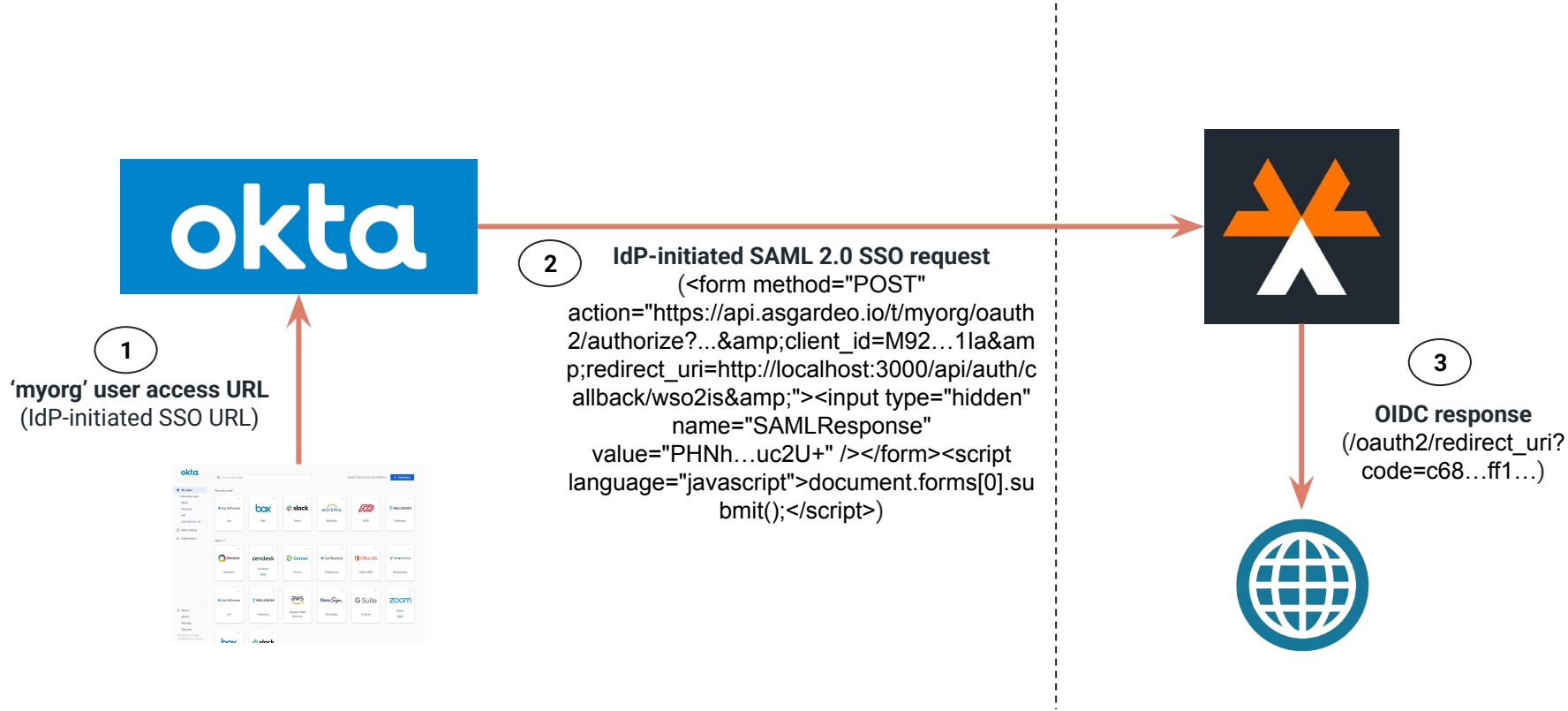
B2B IAM


B2B SaaS Provider
Platform Admin
Admin Privileges
Reseller
Admin Privileges
Reseller Admin
Customer a
Customer b
Customer x
Customer n
Self-register
Customer Admin
Employee
Customer Admin
Employee
User Mgt Privileges
Entitlements Mgt Privileges
Admin-led onboarding
Customer Admin
Employee
Customer Admin
Employee
UN/PW
Enterprise IdP
Branded UN/PW
Passwordless
Customers

OICD Service Provider initiated SSO with SAML 2.0 Federated IdP



SAML 2.0 Federated IdP-initiated SSO with OIDC Application



Summary

Summary of IAM Evolution

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

Question Time!

