Token Enrichment for Identity Providers (IDPs)

Identity-aware security, powered by Policy-Based Access Control (PBAC)

plainID

Dynamic Authorization with Identity-centric Context and Risk-based Signals

OIDC is the industry standard for Single Sign-On (SSO), but its reliance on static claims tied to siloed data leaves organizations unable to adapt to changing contexts. This inflexibility undermines principles like Zero Trust and Least Privileged Access, increasing the risk of unauthorized access through over-privileged access.

PlainID & Existing IDPs: Better Together

Enterprises can address these gaps by combining their existing Identity Provider (IDP) with **PlainID's Dynamic Authorization Service™** for **Token Enrichment**. This integration transforms how permissions are managed, enhancing static claims with real-time, contextual information from multiple identity and organizational data sources.

After a user authenticates, PlainID enhances the access token with additional claims, that are a result of dynamic decisions governed by policies, and supported by data beyond what the IDP stores. This enriched token enables real-time, context-aware access decisions based on factors like time, security events, and risk levels. Applications, APIs, and services use these tokens to enforce consistent authorization policies across all environments, ensuring access is dynamically tailored to minimize risk.

Benefits of the Combined Approach

Integrating PlainID with an existing IDP offers numerous advantages for enterprise security and operational efficiency:

- **Policy-based Access Control:** Adopt PBAC alongside identity management to better define and control the connection between identities and what they can do and access.
- **Real-Time Decisioning:** Dynamic tokens adapt to changing conditions, minimizing risks and enforcing Zero Trust.
- **Improved Visibility and Consistency:** Centralize Authorization across platforms and applications to make it easier for security teams to manage and refine access policies.
- **Enhanced Business Agility:** Create plain language, business friendly dynamic access control policies and reduce the number of policies needed to reduce the burden on IT.

Business Impact

✓ **Support Modern Architecture**
Meet your organization's Identity--first business strategy and user experience.

✓ **Minimize Risk With Identity-First Security**
Address Zero Trust and continuous Authorization in real-time, with context and consistency.

✓ **Better Manage Application Access**
Secure applications and digital assets by dynamically controlling claims based on risk and context.

✓ **Accelerate Time To Market**
Remove dependency on coded authorization, by externalizing to a user-friendly management GUI and expediting the overall process.

Technical Insight

Token Exchange & Token Enrichment

Use API and service mesh Authorizers to exchange application tokens for microservice or API-specific tokens, ensuring tailored, secure access for your applications and APIs – powered by PBAC.

How PlainID Token Enrichment Works

1. User Authenticates to the IDP

2. IDP calls out to PlainID and request which claims and claims values the user is authorized to have

3. Claims are added to the JWT

4. JWT is signed and provided to the application.
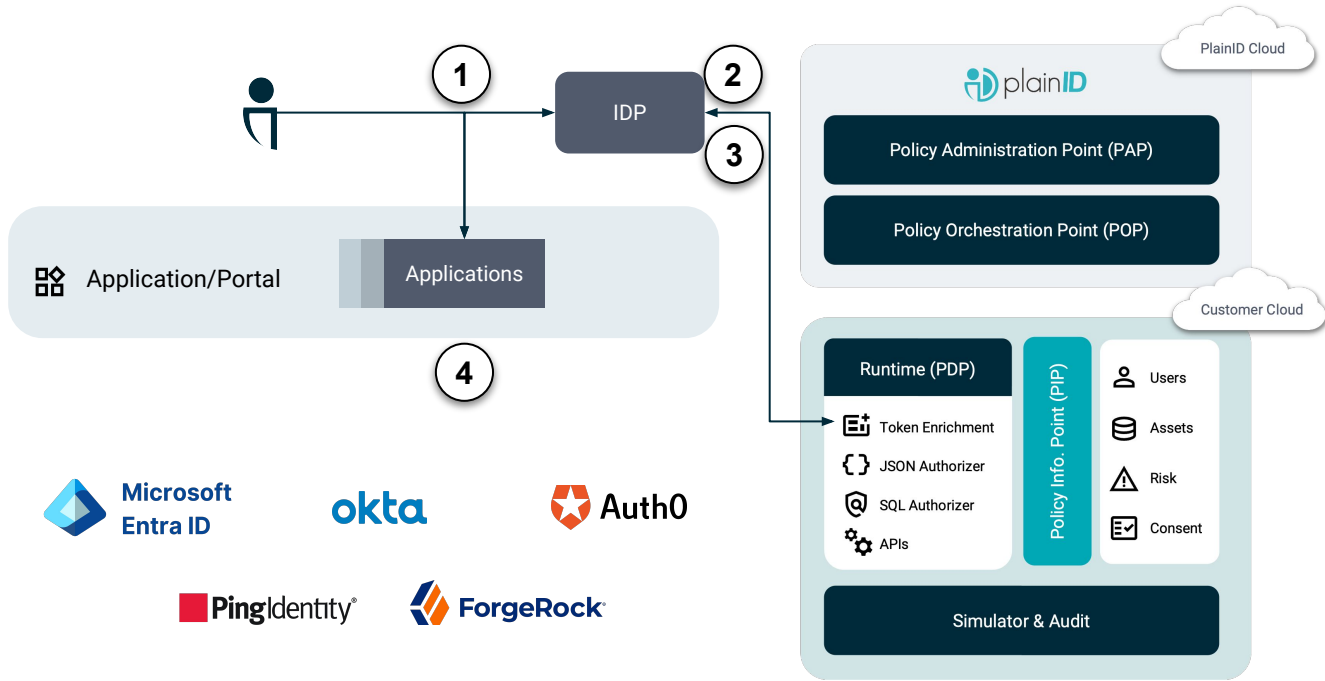
Future-proof Your Enterprise

The **PlainID Integration Hub** is designed to address the complex challenges of enterprise access control. By offering out-of-the-box Authorizers^{TM} and Integrations, it allows for a standardized approach across varied and distributed infrastructures – unifying disparate access controls under one platform.

Visit PlainID.com/integration-hub for more information