Dynamic Authorization Service™ for IDP Token Enrichment

Authorize digital interactions, at scale, extend identity security enterprise-wide

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

OAUTH is the industry standard for Single Sign On (SSO) and enterprises typically rely on claims to inform an application on user permissions. However, claims are the least dynamic approach and does not align with Zero Trust principles.

Claims must be dynamic and contextual. Its permissions cannot be based on siloed identity information alone. Security best practices demands enterprises reduce access dynamically to better address least privileged access.

The PlainID Dynamic Authorization Service™ enriches tokens with claims by using multiple identity data sources. It gives organizations a way to make claims based on identity information known to the IDP as well as identity information from other parts of the organization. **Token Enrichment** combines identity information with contextual risk-based information to determine whether access associated with that claim should be granted, in real-time.

Utilizing **PlainID Dynamic Authorization Service** for Token Enrichment over claims empowers enterprise security and IAM stakeholders with comprehensive authority over Authorization. This control extends to the enforcement of access, whether it occurs in the application or service layer through **PlainID Authorizers™**, or is based on claims within a token. Improve your Identity Security posture through consistency, standardization and visibility of user and service-to-service access.

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
A user-friendly GUI and policy creation using natural language saves developer time and resources.

Features

BUSINESS-DRIVEN API POLICY MANAGEMENT
Leverage a graphical UI management console to express policies in accessible, business-oriented language.

IDENTITY-AWARE ACCESS CONTROL
Apply identity contextual data to authorization enforcement where decisions are based on the true identity rather than highly privileged system accounts.

DYNAMIC & FINE-GRAINED AUTHORIZATION
Calculate policy-defined API access decisions in real-time for continuous permit/deny enforcement.

TOKEN EXCHANGE AND TOKEN ENRICHMENT
Enrich access token by injecting authorization claims into the request header, or mint a new access token containing only relevant information for the transaction using PlainID's Authorization Server.

Key Components of PlainID Dynamic Authorization Service

POLICY DECISION POINT (PDP)
Calculates real-time access decisions based on PAP-defined policies.

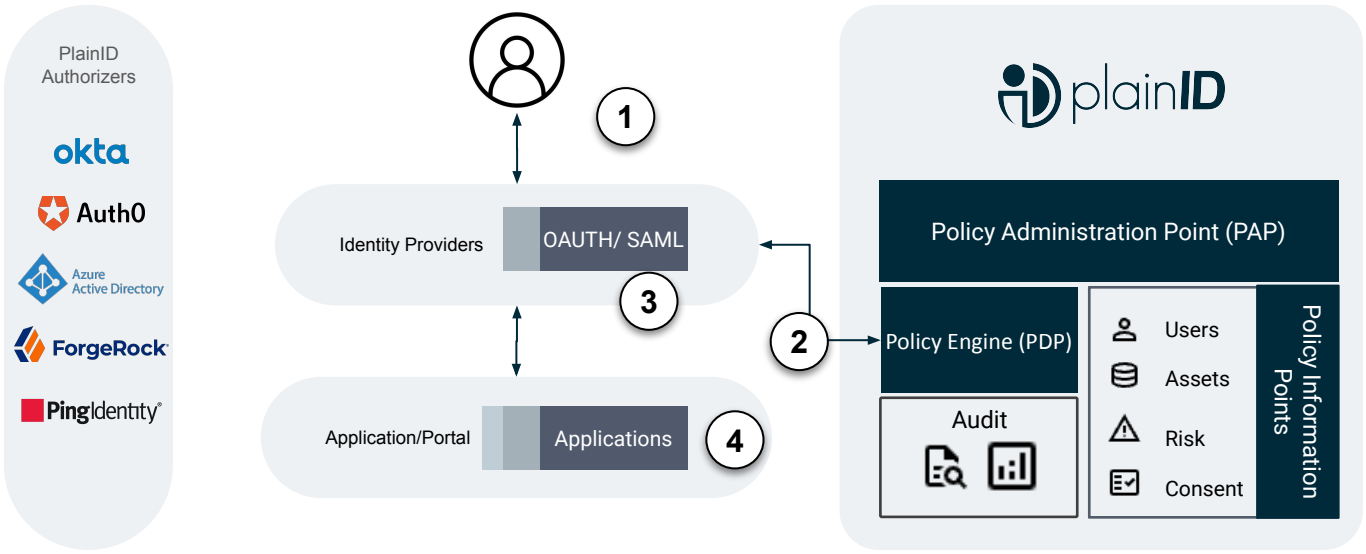
POLICY INFORMATION POINT (PIP)
Collects information on users and assets to support fine-grained decisions.

POLICY ADMINISTRATION POINT (PAP)
Creates and manages the full policy lifecycle. The PAP interface is purpose-built for both technical and business-oriented users.

PLAINID AUTHORIZERS
Ready-to-use integrations to enforce the access decisions for industry-leading API Gateway solutions. Authorizers are also available for securing microservices, data, and applications.

How PlainID Token Enrichment Works

1. User Authenticates to the IDP
2. IDP calls out to PlainID and request which claims the user is authorized to have
3. Claims are added to the JWT
4. JWT is signed and provided to the application.



ABOUT PLAINID

PlainID is The Identity Security Company™. We help identity-centric enterprises defend themselves from adversaries who use identity-based attacks. Our Identity Security Posture Management Platform provides Identity Insights, SaaS Authorization Management, and Dynamic Authorization Services to create identity-centric security across SaaS, APIs, microservices, apps, and data powered by policy-based access control. Visit PlainID.com for more information.

plainID