

# Dynamic Authorization Service™ for API Gateways



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

## API Access Control

Digital transformation initiatives have led many organizations to take an API-first business strategy. This exposes large volumes of data and resources to numerous identities: workforce, customer, partner, and systems.

API gateways are typically used to manage the traffic generated by API calls, but risks remain. According to OWASP, four out of the top five security risks are now related to identity. The explosion of human-to-human and machine-to-machine communication has made secure access to APIs a top priority.

The **PlainID Dynamic Authorization Service™**, part of the **PlainID Identity Security Posture Management Platform™**, provides fine-grained and dynamic access policies for API gateways. **PlainID Authorizers™** provide out-of-the-box integration that simplifies authorization across the enterprise.

## 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.



**API DISCOVERY FOR SWAGGER AND OPENAPI**  
Streamline API access policy creation and enable API discovery for Swagger and OpenAPIs for simplified modeling of underlying assets and asset attributes.

## Business Impact



### SUPPORT MODERN ARCHITECTURE

Meet your organization's API-first business strategy and user experience.



### MINIMIZE RISK WITH IDENTITY-FIRST SECURITY

Address Zero Trust and continuous authorization in real-time.



### BETTER MANAGE API ACCESS TO POLICIES

Secure APIs through a single pane of glass with a central management platform



### ACCELERATE TIME TO MARKET

A user-friendly GUI saves your developers' time and resources.

# Key Components of PlainID's 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)

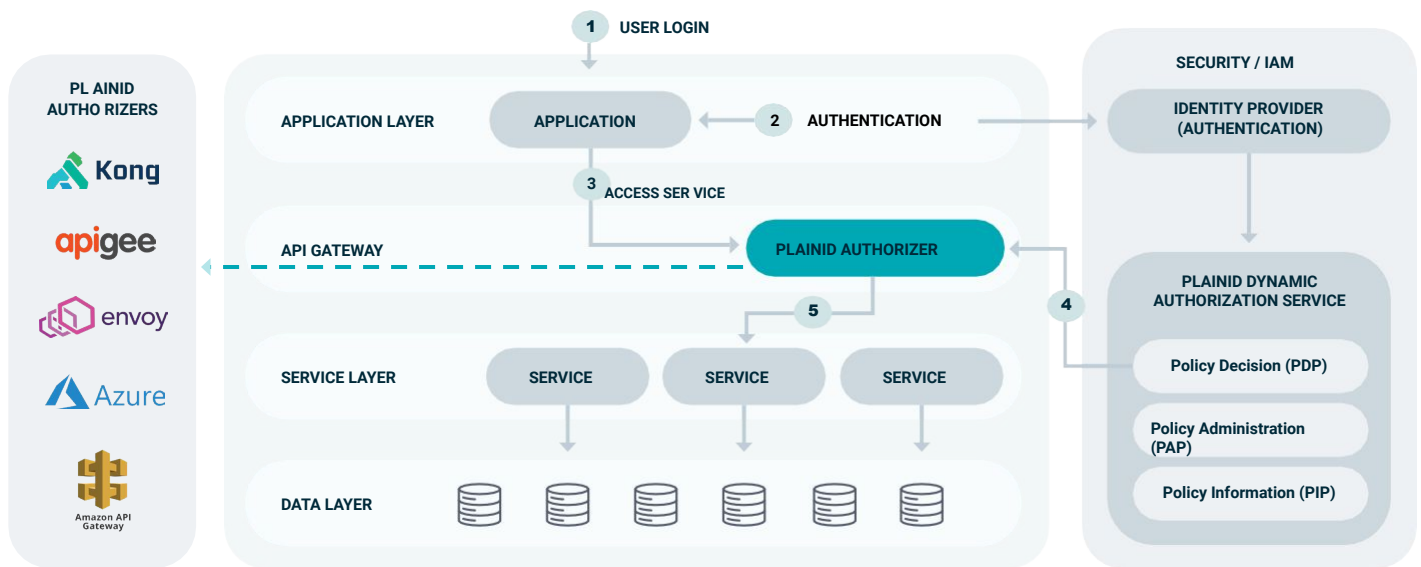
Creates and manages the full policy lifecycle. The PAP interface is purpose-built for both technical and business-oriented users.

## 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.

## Solution Architecture

- 1 User logs into the application
- 2 Application sends authentication request to the Identity Provider (IdP)
- 3 The application sends API calls directed through the API Gateway to access different services
- 4 PlainID's Authorizer (implemented as a plugin in the API Gateway) receives the request and makes a dynamic access decision in real-time, based on the policies. The decision can permit/deny the transaction OR equip the transaction with token exchange/enrichment for additional identity-aware permissions.
- 5 The API call is passed on to the service layer



Visit [PlainID.com](https://PlainID.com) for the full list of authorizers.

## ABOUT PLAINID

PlainID is the world's leading provider of enterprise Authorization, helping enterprises address the complex challenges of Identity Security. The PlainID Platform allows you to discover, manage, and authorize access control policies for enterprise applications and data. Our solution is architected to protect against identity-centric security threats powered by Policy-Based Access Control (PBAC). Visit PlainID.com for more information.