plainID
THE AUTHORIZATION COMPANY

Authorization for API Gateways

Securely connecting identities to digital assets, powered by Policy Based Access Control (PBAC)

API Access Control

Digital transformation initiatives have led many organizations to take an API-first business strategy. In doing so, it causes organizations to expose large volumes of data and resources to various types of identities: workforce, customer, partner, and systems.

API gateways are typically used to manage the traffic generated by API calls. However, four out of the top five security risks are now related to identity according to the OWASP API Security Top 10 vulnerabilities. The rapid adoption of APIs has caused an explosion of human-to-human communication, as well as machine-to-machine communication – making secure access to APIs more critical than ever for organizations.

The PlainID Authorization Platform provides fine-grained and dynamic access policies for API gateways and enforces them through the API gateway (North-South traffic). This is done using **PlainID Authorizers**™ which provide out-of-the-box integration with industry leading API gateways to simplify authorization across the enterprise.

Business Values

Support Modern Architecture

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

Minimize Risk with Identity-first Security

Proactively address Zero Trust and continuous authorization in real-time by securely connecting identities to digital assets.

Better Manage API Access Policies

Consistently and continuously secure APIs through API gateways with access policies through a single pane of glass with a central management platform.

Accelerate Time to Market

Save developer time and resources by replacing the need for coding access policies with a user-friendly GUI.

Features:

Business-driven Policy Management for APIs

Leverage a graphical UI management console where API access policies can be quickly and easily configured to reflect business logic using simple 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 API access decisions, as defined by the policies, at the time of the request in real-time for continuous security control.

Permit / Deny Enforcement

Unify authorization enforcement and meet access policy requirements at the API gateway level.

PlainID Authorizers for API Gateways

Integrate dynamic, runtime authorization with ready-to-use authorizers for industry leading API gateway providers such as Apigee, Kong, AWS API Gateway, and more.

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 OpenAPIs

Streamline API access policy creation and enable API discovery for Swagger and OpenAPIs for simplified modeling of underlying assets and asset attributes.

plainID THE AUTHORIZATION COMPANY

Authorization for API Gateways

Securely connecting identities to digital assets, powered by Policy Based Access Control (PBAC)

Solution Architecture

API Gateway Enforcement Through PlainID Authorizers

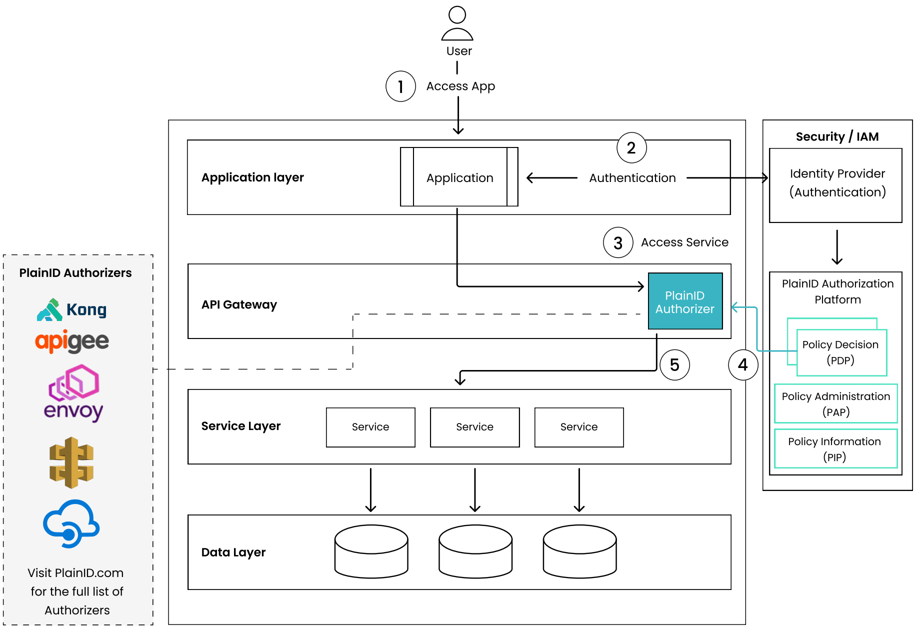
1. User logs into the application

2. Application sends Authentication request to the Identity Provider (IdP)

3. The application sends API calls that are directed through the API Gateway in order to access different services

4. PlainID's Authorizer (implemented as a plugin in the API GW) receives the request and makes a dynamic access decision in real-time, based on the policies.
   The decision can be:
   - Permit or deny the transaction
   - Permit the transaction with token exchange or token enrichment for additional identity-aware context and policy decisions

5. The API call is passed on to the service layer



Key Components of the PlainID Authorization Platform:

- **Policy Decision Point (PDP)** – The PDP component is responsible for calculating access decisions in real-time, based on policies defined in the PAP.

- **Policy Administration Point (PAP)** – The PAP interface is used to create, modify, and manage the full policy lifecycle . It is purpose-built for both techinical and business-oriented users to design and manage policies.

- **Policy Information Point (PIP)** – The PIP component is responsible for collecting information such as attributes on the user and assets from various resources to support fine-grained decisions.

- **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.

About PlainID

PlainID, the Authorization Company, simplifies the complexity businesses face when securely connecting identities to digital assets. Powered by PBAC, PlainID provides a SaaS-based, centralized policy management platform with decentralized enforcement to manage who can access what across the enterprise technology stack; including applications, data, API, microservices and more.

Visit us

plainID THE AUTHORIZATION COMPANY