Authorization for Microservices

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

Dynamic Authorization for Microservices

Larger organizations have hundreds if not thousands of microservices that interact with each other through API calls. The sheer number and complexity of calls between microservices (East-West traffic) can make authorization a security challenge.

Unlike North-South traffic where a single API Gateway is typically secured, requests between microservices must be addressed at scale. An efficient and proactive approach to securing microservices decouples the authorization policy lifecycle management.

The PlainID Authorization Platform provides centralized management with distributed enforcement, where the logic and policies are centrally defined outside of the service, and the enforcement is done locally at the service level. This is done through **PlainID Authorizers**™ which provide out-of-the-box integration (as a sidecar) with industry leading service mesh solutions to simplify authorization across the enterprise.

Business Values

Support Modern Architecture

Scale agile processes to meet your 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.

Unify Microservices Access Policies

Consistently and continuously secure microservices 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 and microservice level.

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.

PlainID Authorizers for Microservices

Integrate dynamic, runtime authorization with ready-to-use authorizers for industry leading service mesh solutions such as Istio, Kuma, Linkerd, and more.

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.

Authorization for Microservices

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

Solution Architecture

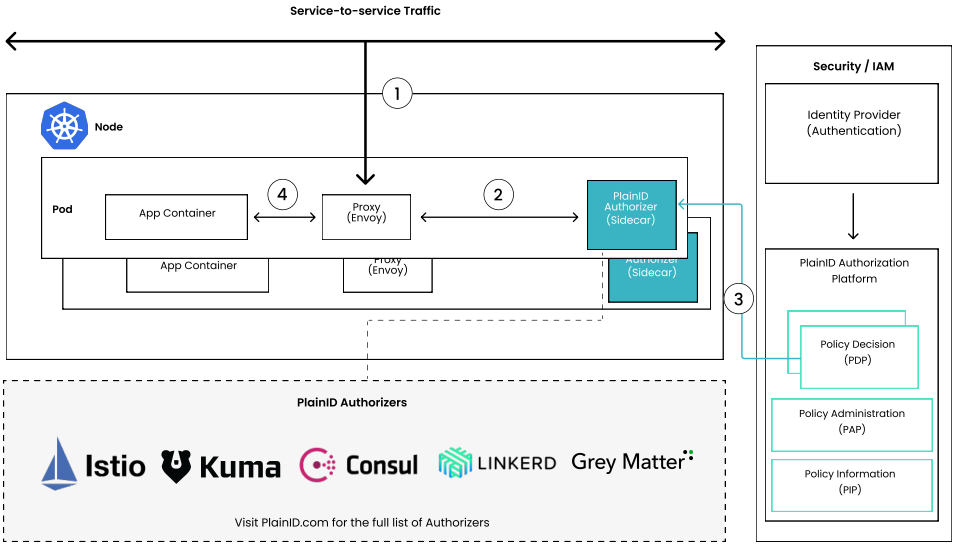
Service-to-Service Enforcement Through PlainID Authorizer

1. The client sends the access/ID token in the request header

2. The request is intercepted by the envoy proxy and passed to the PlainID Authorizer (sidecar) that is automatically injected to the pods as a container.

3. The sidecar can:
   - Permit or Deny the transaction based on the defined policies (the decision is based on the request URL, header, and body)
   - Permit the transaction with token exchange or token enrichment for additional identity-aware context and policy desicions

4. If the authorization decision is permit, the Envoy proxy passes the request to the service container, otherwise, If the authorization decision is deny, the request never reaches the actual service container and a 403 response is returned immediately



Key Components of the PlainID Authorization Platform:

- **Policy Decision Point (PDP)** – The PDP component is responsible for calculatin 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