KubeCon + CloudNativeCon
North America 2026

HITACHI

One Platform for AuthN and AuthZ: Keycloak Meets AuthZEN

Presented by

Yoshiyuki Tabata, Hitachi, Ltd.

Date

November 10, 2026

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Contents

01 What Is Authorization?

02 What Does AuthZEN Standardize?

03 Keycloak Meets AuthZEN

04 Demo: AuthZEN in Practice

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

About Me



Yoshiyuki Tabata

Chief OSS Consultant
Hitachi OSPO

LinkedIn ytabata

X @yo_tabata

GitHub @y-tabata

CNCF TAG Security and Compliance Tech Lead / CNCF Ambassador

- Winner of the 2026 TAGGIE Award
- Published the CNCF IAM Whitepaper
- Participating in the MCP Server Authentication and Authorization Standards Initiative

AAIF Ambassador

- Member of the Identity and Trust Working Group

Keycloak Contributor

- Co-chair of KeycloakCon Japan and KeycloakCon EU

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Chapter 1

What Is Authorization?

01 **What Is Authorization?**

02 What Does AuthZEN Standardize?

03 Keycloak Meets AuthZEN

04 Demo: AuthZEN in Practice

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

What Is Authorization?

Common definitions

Authentication

- Who are you?
- Establishes and verifies the identity of a subject

Authorization

- What are you allowed to do?
- Determines what that subject may do

The definition sounds clear. What do we actually need to build?

The definition alone does not tell us how to implement authorization in a real system.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

The Two Faces of Authorization

Authorization has two faces: granting authority and controlling access.

Delegation



Access Control

Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

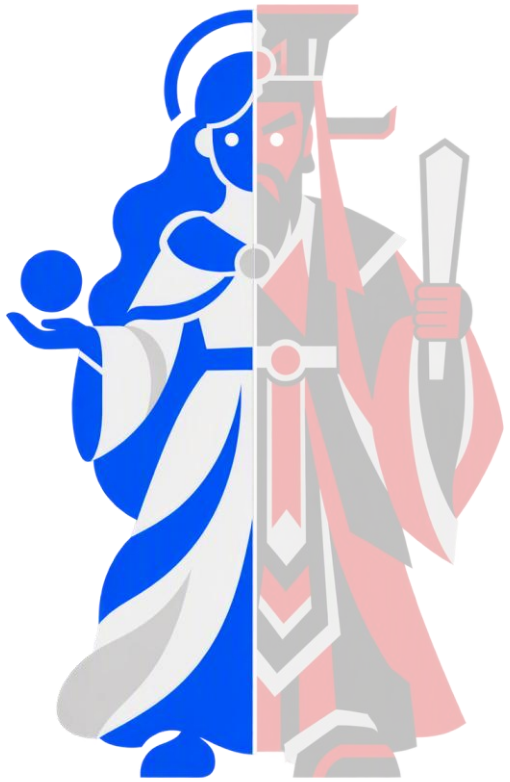
Delegation: Granting Authority

Delegation allows one party to grant another party limited authority to act on its behalf.



Delegation is like a goddess granting a hero special powers.

Delegation Access Control



Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

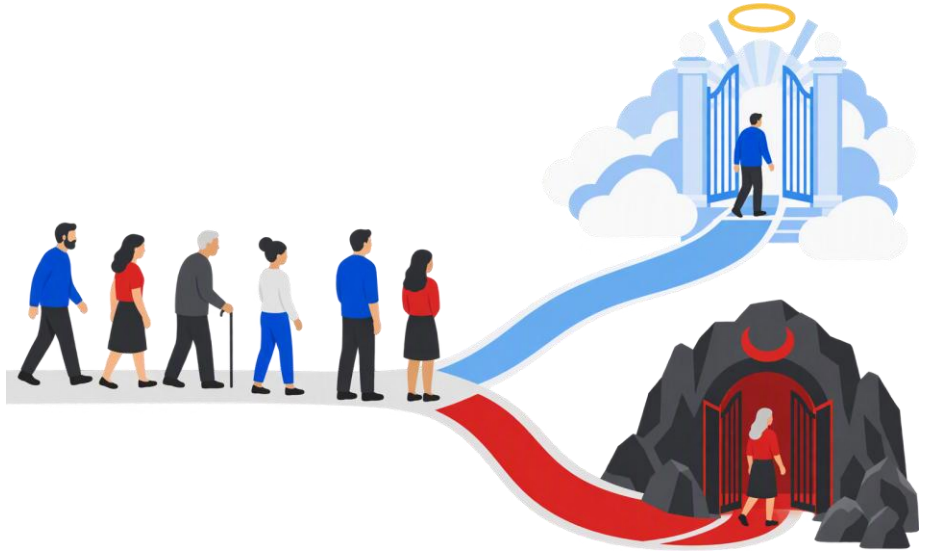
HITACHI

Access Control: Guarding the Gate

Access control determines whether a requested action is allowed at the point of access.

Delegation **Access Control**





Access control is like a gatekeeper deciding who may pass.

Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Authorization Needs Both

Authorization fails if authority is granted too broadly or access is controlled too loosely.



DO NOT grant unlimited authority

- A god-tier cheat skill granted without limits defeats every gate

Delegation **Access Control**





DO NOT let everyone pass

- A gatekeeper who lets everyone pass defeats every limit

Authorization requires both proper delegation and effective access control.

Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Authorization Is Already Critical for APIs

Authorization failures remain among the most critical security risks for modern APIs.

In the OWASP API Security Top 10 (2023), three of the top five risks are authorization failures.

API1	Broken Object Level Authorization
API3	Broken Object Property Level Authorization
API5	Broken Function Level Authorization

Authenticating the client is not enough. Every request needs a decision: who may perform which operation on which resource.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

AI Agents Make Authorization More Important

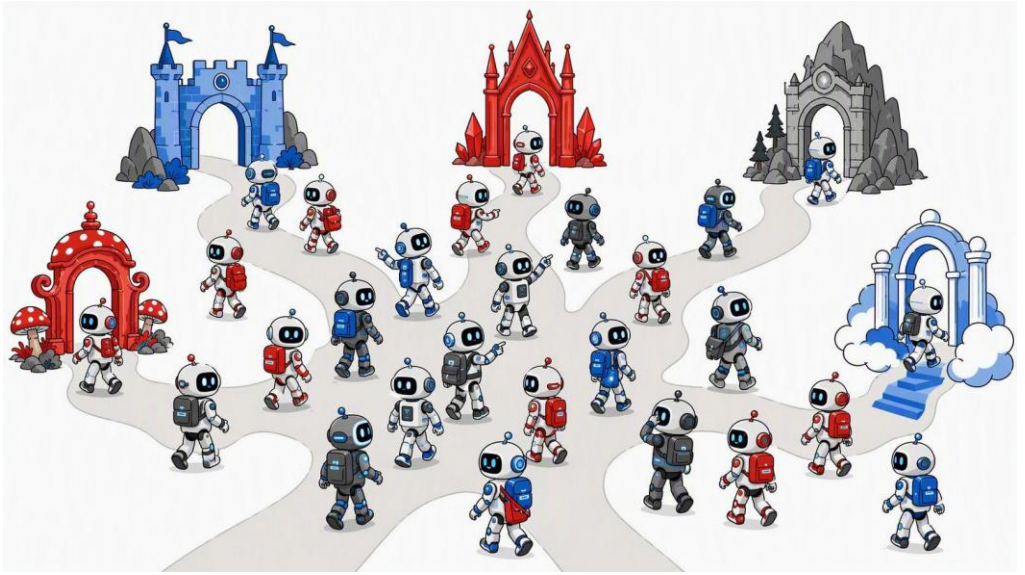
AI agents bring more clients and more dynamic interactions with APIs and tools.

Traditional API Clients



A relatively small set of known clients
Predefined API integrations
Known operations

AI Agents



Many distributed agents
Dynamic tool discovery
Tool selection at runtime

Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Chapter 2

What Does AuthZEN Standardize?

01 What Is Authorization?

02 **What Does AuthZEN Standardize?**

03 Keycloak Meets AuthZEN

04 Demo: AuthZEN in Practice

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

AuthZEN Focuses on Access Control

AuthZEN focuses on the access control side of authorization.

OAuth and related specifications standardize how limited access is delegated to a client.

Delegation | Access Control



AuthZEN standardizes how authorization decisions are requested and returned.

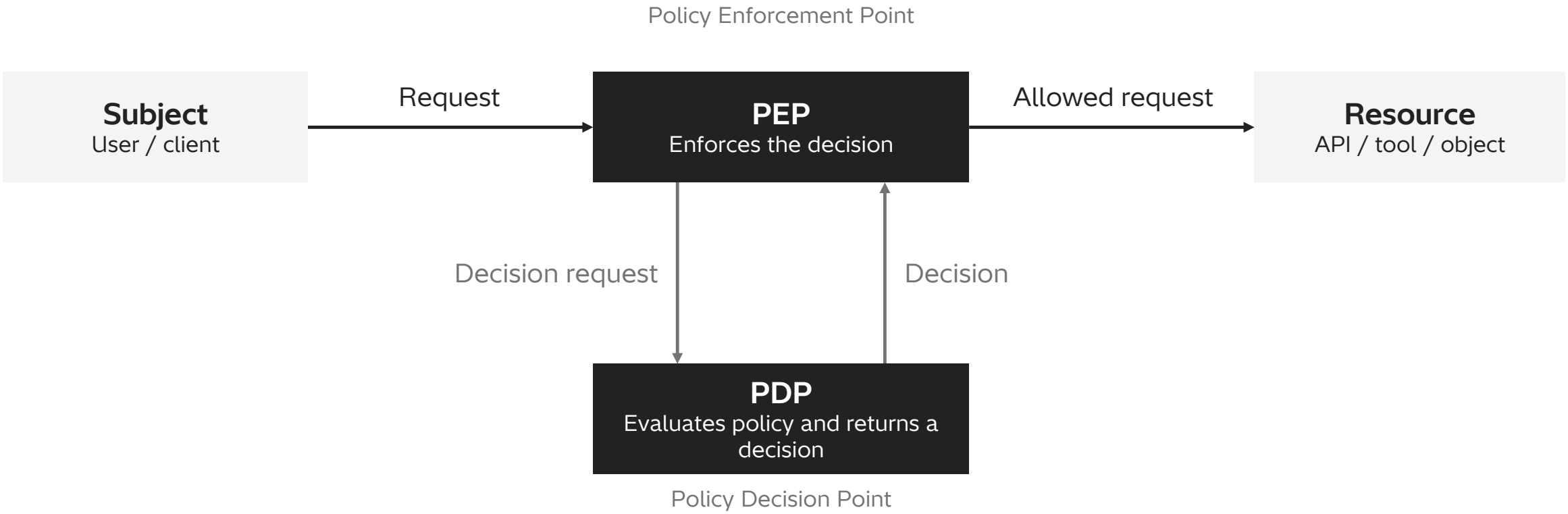
Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Separating Decision from Enforcement

A common authorization architecture separates policy decision-making from enforcement at each access boundary.



Without this separation, authorization logic is duplicated across applications, policies become inconsistent, audits become harder, and policy changes require application changes.

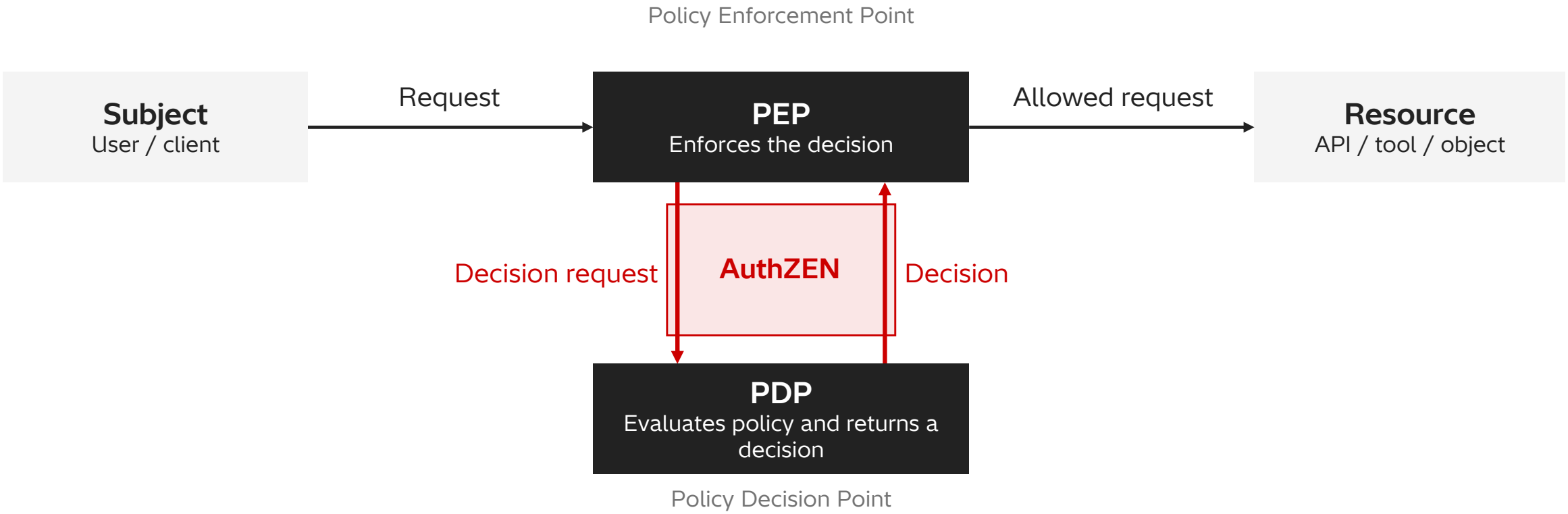
Reference: NIST SP 800-162 (ABAC)

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

AuthZEN Standardizes the PEP-to-PDP Interface

AuthZEN defines how a PEP requests an authorization decision from a PDP.



A standard interface decouples PEP and PDP implementations.

Reduces dependence on product-specific APIs and improves interoperability across policy engines.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Access Evaluation API

The Access Evaluation API asks whether a subject may perform an action on a resource.

Subject Who is attempting the action?

Action What are they attempting to do?

Resource What are they attempting to access?

Context (optional) Under what circumstances?

The PDP evaluates the request against policy and returns a decision.

Request

```
{
  "subject":  { "type": "user", "id": "alice" },
  "action":   { "name": "invoke" },
  "resource": { "type": "mcp-tool",
                "id": "delete-file" },
  "context":  {}
}
```

Response

```
{
  "decision": true
}
```

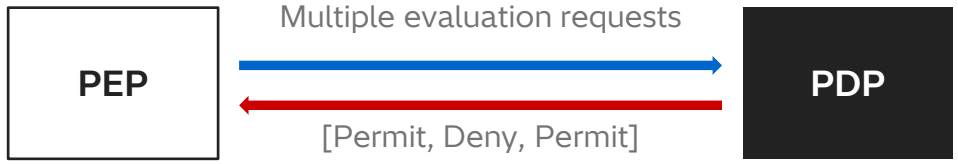
© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Beyond a Single Decision

Batch decisions, find permitted subjects / resources / actions, and discover the PDP.

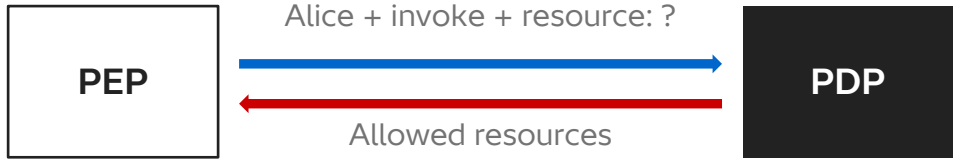
Evaluate in batch



Access Evaluations API

Evaluate multiple requests in one API call.

Search

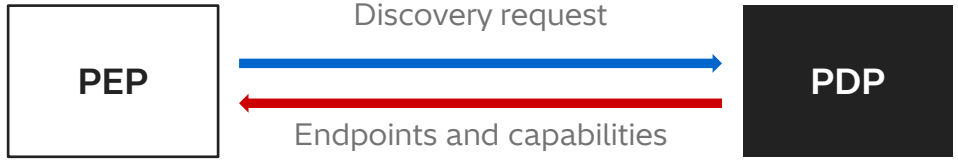


Search API

Find permitted subjects, resources, or actions.

Example is Resource Search API

Discover



PDP Discovery

The PEP learns where the PDP is and what it supports.

© Hitachi, Ltd. 2026. All rights reserved.

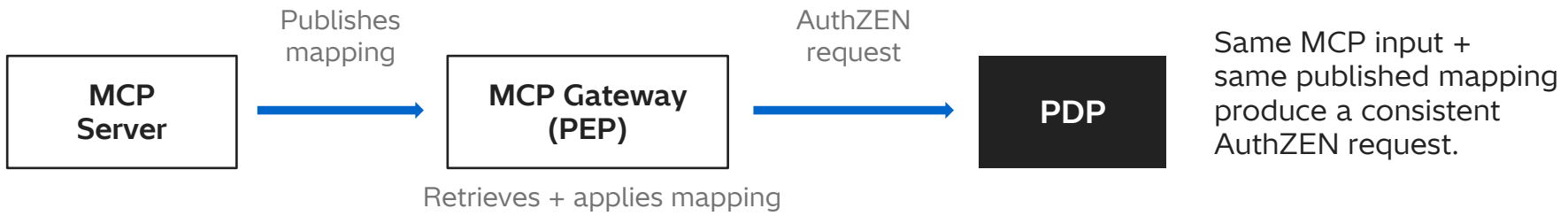
HITACHI

AuthZEN Extensions for Agentic Authorization

Extend request mapping and decision handling so agents can use tools consistently and safely.

Map

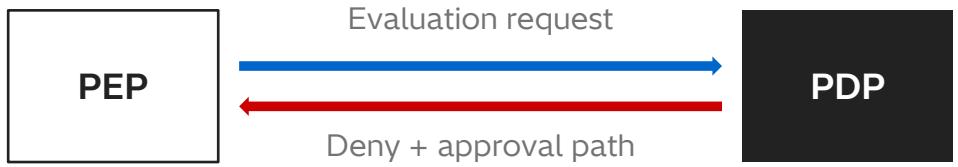
COAZ + COAZ-MCP



Same MCP input + same published mapping produce a consistent AuthZEN request.

COAZ defines the mapping model. COAZ-MCP defines MCP defaults and server-declared mappings.

Request approval

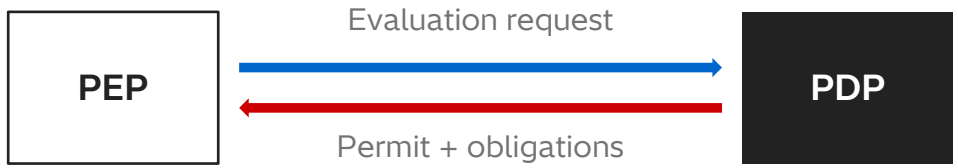


Access Request and Approval Profile

Conditional denial: request approval, then re-evaluate.

Example: pause a refund for approval.

Fulfill duties



Profile for Obligations

Conditional permission: the PEP must fulfill required duties.

Example: log the tool call before allowing execution.

Emerging profiles published as separate Working Group Drafts.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Chapter 3

Keycloak Meets AuthZEN

01 What Is Authorization?

02 What Does AuthZEN Standardize?

03 **Keycloak Meets AuthZEN**

04 Demo: AuthZEN in Practice

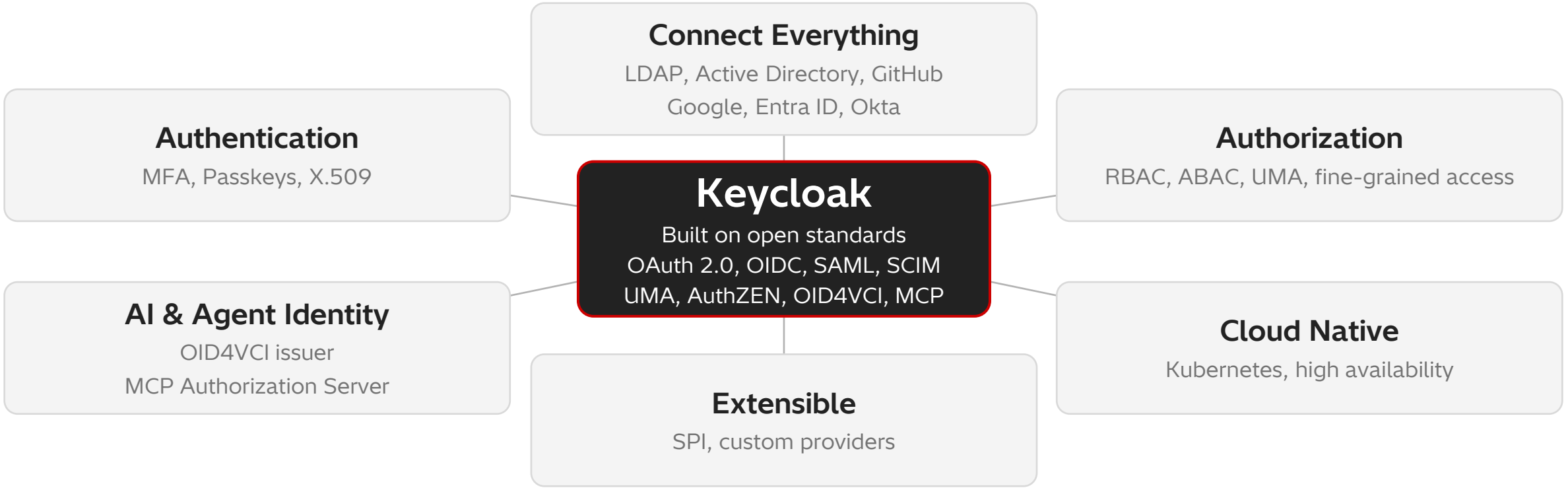
© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

What Is Keycloak?

Open source Identity and Access Management (IAM) platform

A CNCF incubating project providing OAuth 2.0 Authorization Server and authentication capabilities.



Keycloak 26.7.0: experimental OpenID AuthZEN Authorization API 1.0 support

Exposes standard AuthZEN Evaluation and Evaluations APIs. Acts as a PDP for single and batch authorization decisions.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

When Delegation and Access Control Live Apart

Delegation and access control are often implemented by separate platforms.



Identity Provider / Authorization Server

Authentication + Delegation

Authentication and Single Sign-On
Identity management
OAuth 2.0 / OpenID Connect
Token issuance

User IDs, roles, attributes and scopes

Synchronize & map

IDs / roles
attributes / scopes

Policy Engine



Access Control

Resources, scopes, policies and permissions
Fine-grained authorization
Policy Decision Point
AuthZEN Evaluation / Evaluations APIs

User IDs, roles, attributes and scopes

Shared identities, roles, attributes, and scopes require synchronization and semantic alignment.

Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

One Platform for AuthN and AuthZ

Keycloak brings authentication, delegation, and access control together on one platform.

Keycloak

Authentication + Delegation

Authentication and Single Sign-On
Identity management
OAuth 2.0 / OpenID Connect
Token issuance



Access Control

Resources, scopes, policies and permissions
Fine-grained authorization
Policy Decision Point
AuthZEN Evaluation / Evaluations APIs

Shared identities, roles, attributes and scopes

One platform. No additional cross-product identity sync or mapping.

Token issuance and access decisions use the same identity data inside Keycloak.

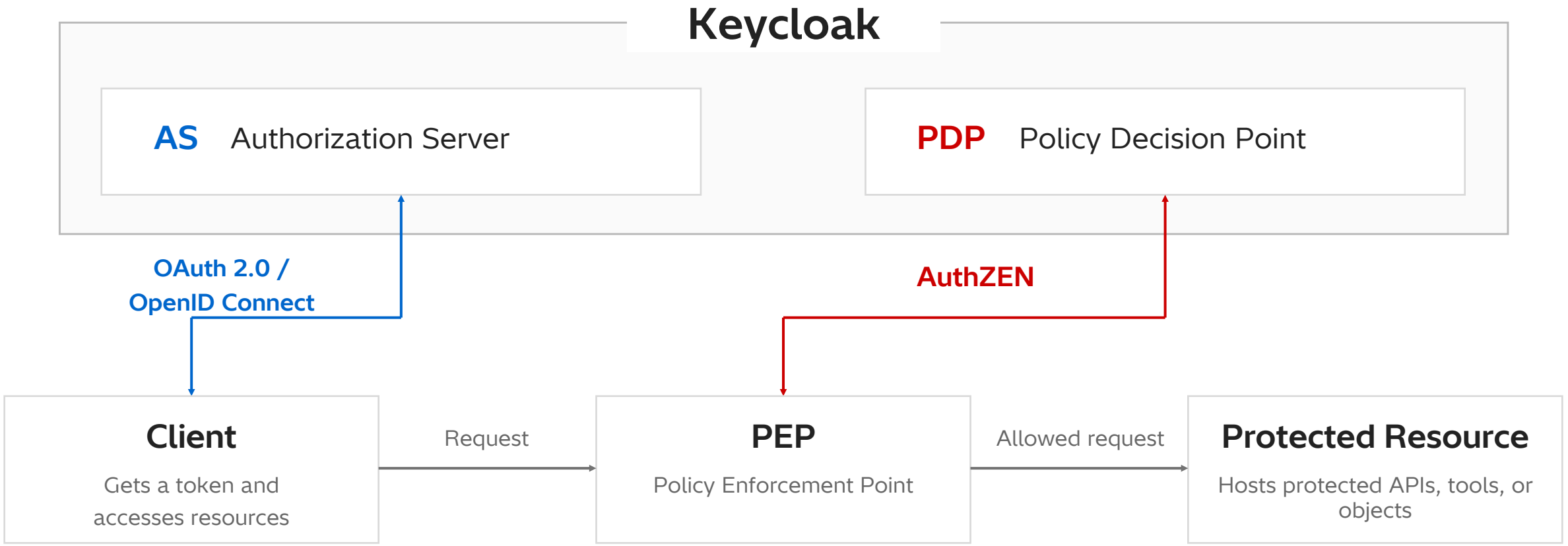
Illustrations generated with AI.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

One Platform Architecture

Keycloak acts as both the Authorization Server and the Policy Decision Point.



OAuth 2.0 / OpenID Connect connects the client to the Authorization Server. AuthZEN connects the PEP to the PDP.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Chapter 4

Demo: AuthZEN in Practice

01 What Is Authorization?

02 What Does AuthZEN Standardize?

03 Keycloak Meets AuthZEN

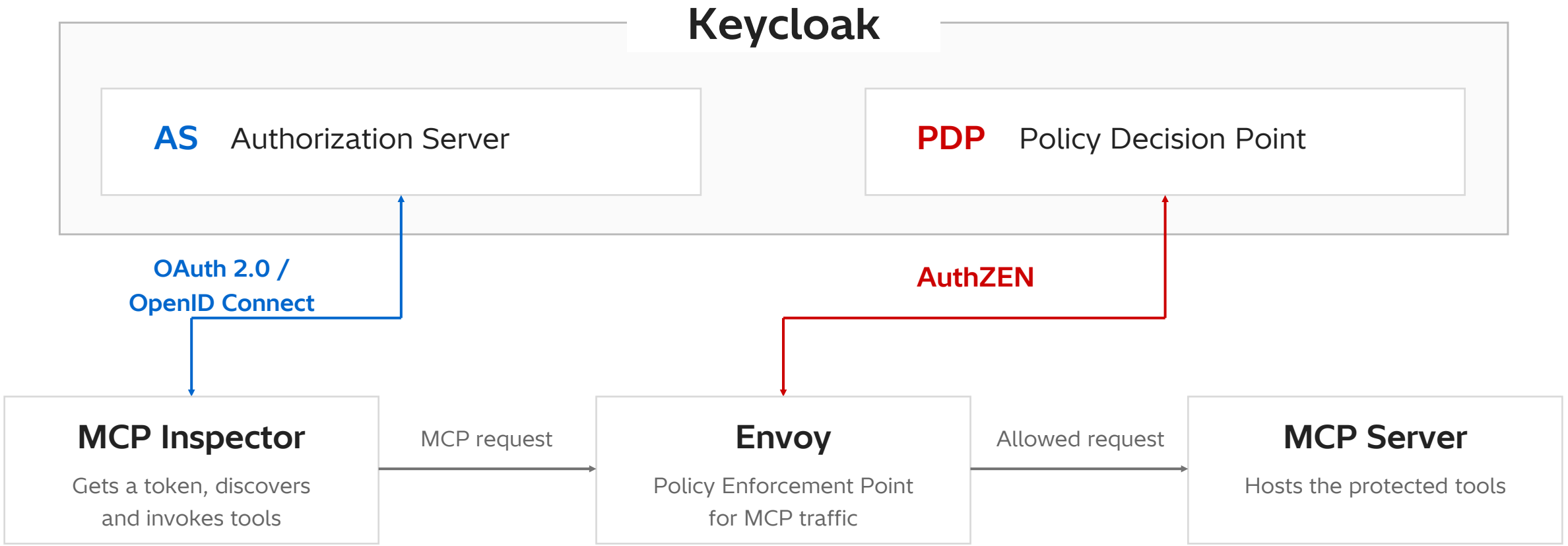
04 **Demo: AuthZEN in Practice**

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Demo Architecture

Envoy enforces authorization for MCP tool calls using decisions from Keycloak through AuthZEN.



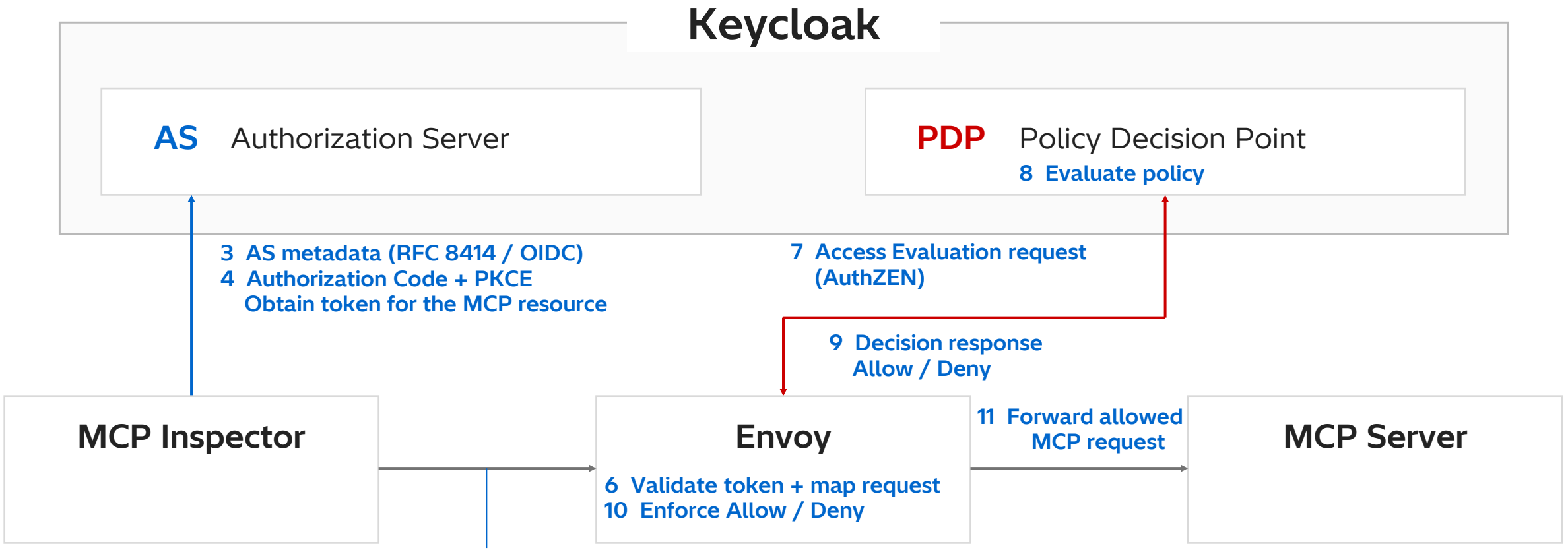
OAuth / OpenID Connect connects the MCP client to the AS. AuthZEN connects the PEP to the PDP.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Demo Scenario

OAuth token issuance and AuthZEN-based authorization decisions build on the same identity data in Keycloak.



Demo & materials

https://github.com/Hitachi/oss-assets/tree/main/sessions/2026/kubecon-na/authzen

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Demo

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Key Takeaways

1

Authorization has two faces

Delegation grants authority. Access control enforces it.

2

AuthZEN standardizes the PEP-to-PDP interface

PEPs can interoperate with different policy engines through a common authorization interface.

3

Keycloak is one platform for AuthN and AuthZ

Authentication, OAuth-based delegation, and AuthZEN-based access control in a single open source platform.

Feedback

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI

Trademarks

- OpenID® is a trademark (registered in numerous countries) of the OpenID Foundation.
- CloudNativeCon®, CNCF®, Envoy® and KubeCon® are registered trademarks of The Linux Foundation in the United States and/or other countries.
- Model Context Protocol® is a registered trademark of LF Projects, LLC.
- OWASP® is a service mark of OWASP Foundation, Inc. in the United States and other countries.
- Other company names, product names and service names mentioned herein may be trademarks or registered trademarks of their respective owners.

© Hitachi, Ltd. 2026. All rights reserved.

HITACHI