AuthZEN: The “OpenID Connect” of Authorization

Gartner IAM Summit 2025

Homan Farahmand
VP Analyst, Gartner

Omri Gazitt
Co-founder, Aserto

David Brossard
CTO, Axiomatics

OpenID®

State of IAM

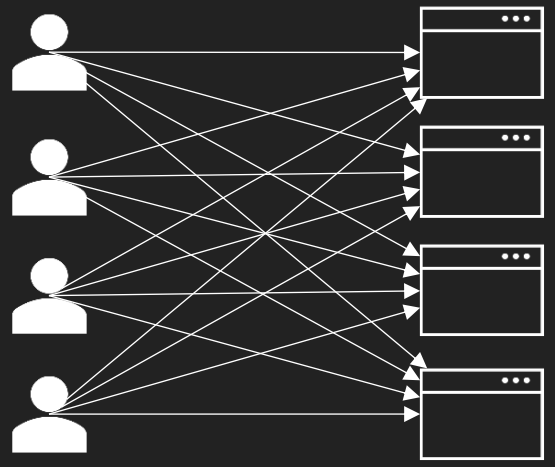
Authentication is “solved”

- OAuth2, OIDC, SAML, JWT
- Workforce SSO: Okta, Entra, Ping Identity, …
- CIAM: Auth0, Cognito, AAD B2C, …

“n + m” problem

Authorization is broken: #1

- No standards or protocols (yet)
- Each app bakes-in domain-specific AuthZ
- Overprovisioned static roles, spaghetti code



“n * m” problem

OpenID AuthZEN Vision

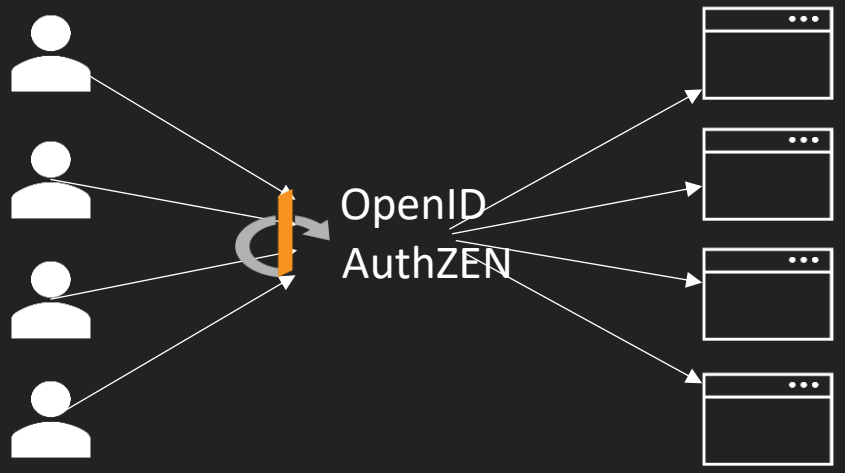
Authentication is “solved”

- OAuth2, OIDC, SAML, JWT
- Workforce SSO: Okta, Entra, PingID, …
- CIAM: Auth0, Cognito, AAD B2C, …

“n + m” problem

Authorization is like authentication

- AuthZEN PEP-PDP API
- Each app externalizes authorization to PDP
- Commercial Workforce and CIAM solutions



“n + m” problem

OpenID®

What is modern authorization?

	Traditional	Modern	
WHAT	Coarse-grained, tenant-level permissions (RBAC)	**Fine-grained**: resource-level permissions (ABAC, ReBAC)	Principle of least privilege
HOW	Authorization “spaghetti logic” embedded in the application	**Policy-based**: authorization logic extracted out of the application	Separation of duties
WHEN	Permissions evaluated at login time, scopes embedded in access token	**Real-time**: permissions evaluated before granting access to resource	Continuous enforcement

Modern authorization

Ecosystems, standards, & OSS

Policy as code (ABAC)

Policy as data (ReBAC)

XACML
2001


ALFA
2014


AuthZEN
2024


Zanzibar
2020

NGAC
2016


Open Policy Agent


Casbin


TOPAZ


OpenFGA™


spicedb


cerbos

CEDAR

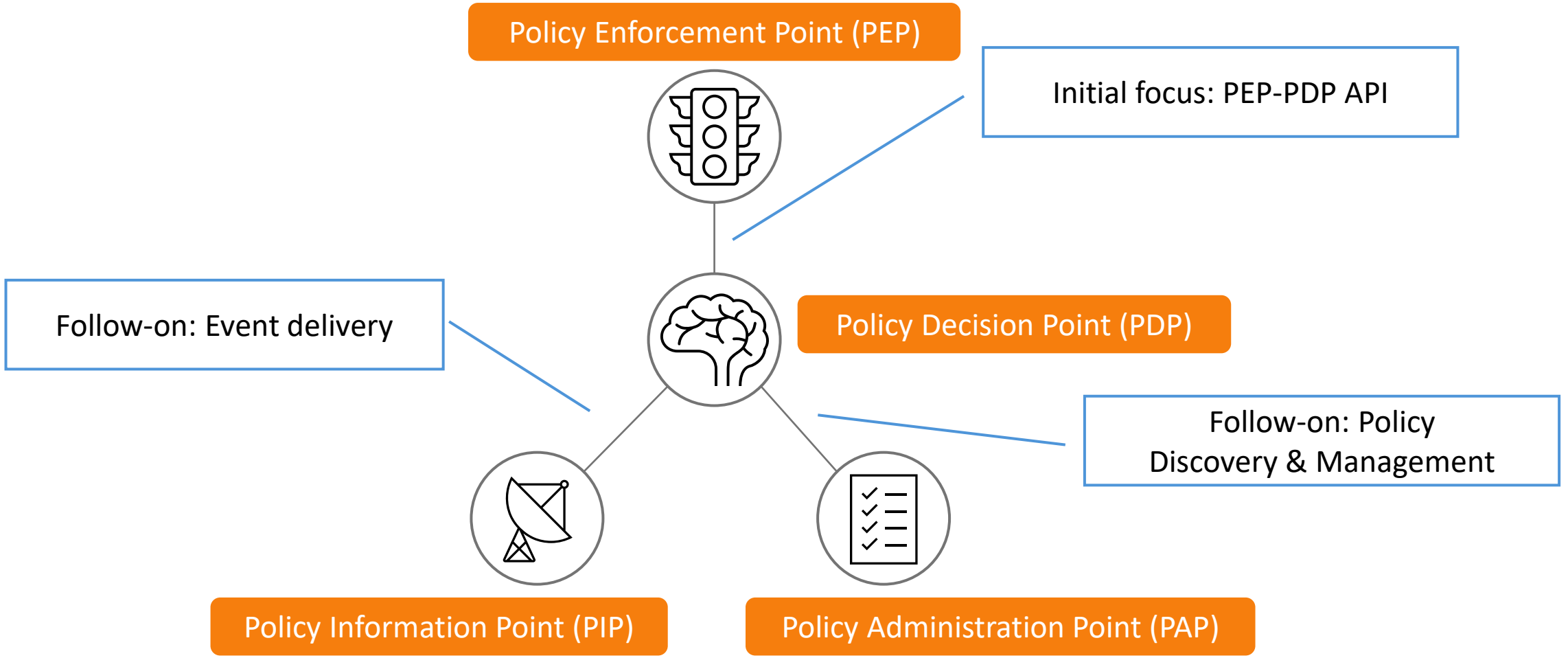

ORY


OSO

OpenID

The AuthZEN Charter

https://openid.net/wg/authzen/



AuthZEN 1.0 Implementer's Draft

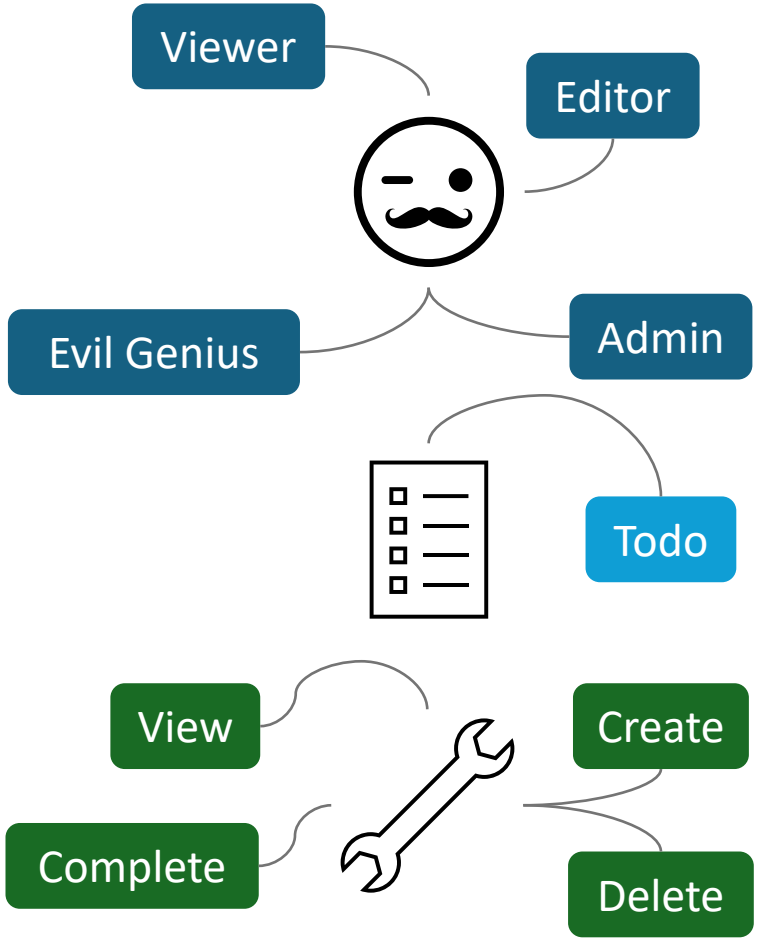
https://openid.github.io/authzen/

```
{
  "subject": {
    "type": "user",
    "id": "CiRm…2Fs"
  },
  "action": {
    "name": "can_delete_todo"
  },
  "resource": {
    "type": "todo",
    "id": "1"
    "properties": {
      "ownerID": "beth@the-smiths.com"
    }
  }
}
```

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

First interop use-case: Todo application

https://authzen-interop.net/docs/scenarios/todo



Todo Application

This document lists the request and response payloads for each of the API requests in the Todo interop scenario.

> TIP
> This is a copy of the payload document defined by the AuthZEN WG. The definitive document can be found here.

Overview of the scenario

The Todo application manages a shared todo list between a set of users.

There are 5 actions that the Todo application supports, each with a permission associated with it:

Action	Permission
View a user's information	`can_read_user`
View all Todos	`can_read_todos`
Create a Todo	`can_create_todo`
(Un)complete a Todo	`can_update_todo`
Delete a Todo	`can_delete_todo`

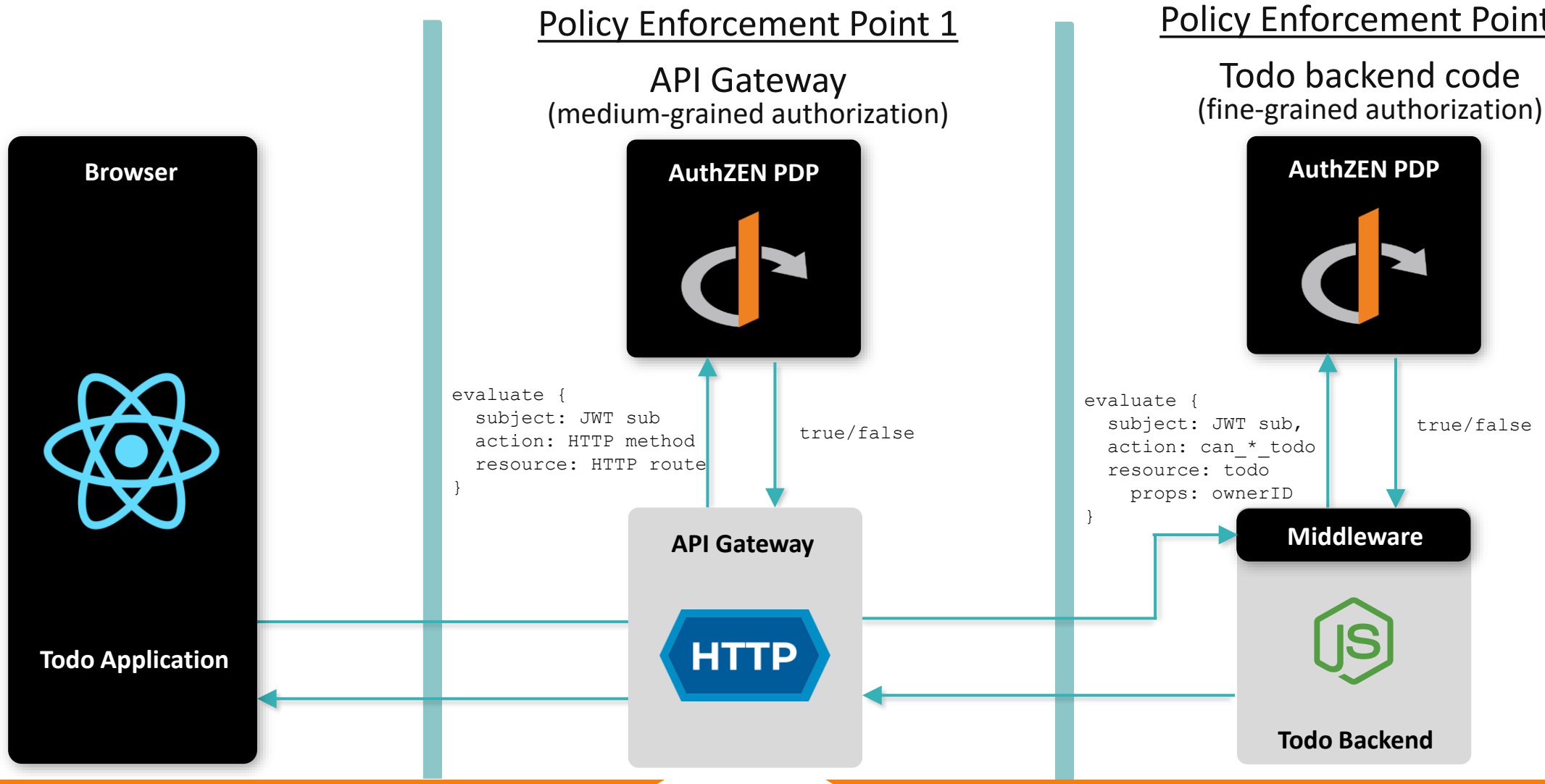
There are four roles defined:

- `viewer` - able to view the shared todo list (`can_read_todos`), as well as information about each of the owners of a Todo (notably, their picture) (`can_read_user`)
- `editor` - `viewer` + the ability to create new Todos (`can_create_todo`), as well as edit and delete Todos *that are owned by that user*
- `admin` - `editor` + the ability to delete any Todos (`can_delete_todo`)
- `evil_genius` - `editor` + the ability to edit Todos that don't belong to the user (`can_update_todo`)

There are 5 users defined (based on the "Rick & Morty" cartoon), each with one (or more) roles, defined below in the Subjects section.

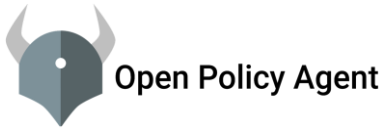
Interop architecture and demo

https://authzen-topaz-proxy.demo.aserto.com



Interoperable implementations (Dec 2024)

Compliant with: Draft 02, Implementers Draft 01, Preview Draft 00



Compliant with: Preview Draft 00

Interoperable implementations (March 2025)

Policy Decision Points

Aserto
AXIOMATICS
aws
CEDAR
cerbos
empowerID
INDY KITE
okta
OpenFGA™
Open Policy Agent
Permit.io
Ping Identity
plainID
Rock Solid Knowledge
sgnl
STRATA
THALES
TOPAZ

API Gateways

Amazon API Gateway
BROADCOM
envoy
Kong
Tyk
WSO2
zuplo

2025 Roadmap

AuthZEN 1.0 Core:

- `/evaluation` endpoint: Draft 01 (Implementer's Draft – Nov 2024)
- `/evaluations` endpoint: Draft 02 (Jan 2025)
- `/search/{subject,resource,action}`: Draft 03 (Feb 2025)
- Discovery mechanism: Draft 04 (anticipated April 2025, ID 2)
- Final Specification: Summer/Fall 2025

On the roadmap:

- AuthZEN 1.0 API Gateway Profile: Summer 2025
- AuthZEN 1.0 Event Delivery (via Shared Signals profile): Fall 2025
- AuthZEN 1.0 IDP Profile: Fall 2025

Call to Action

- Attend one or more of the AuthZEN interop showcase sessions this afternoon: 13:00, 14:45, 16:30 in the Italian Room (ground floor next to Peninsula B)
- Create an AuthZEN-based Authorization Control Plane for your enterprise (just like you did for OpenID-based SSO)
- Externalize the authorization for your internal apps whenever possible
- Encourage your SaaS vendors to become AuthZEN-compliant and plug into your Authorization Control Plane

Where to find us

- AuthZEN mailing list: https://openid.net/wg/authzen
- GitHub: https://github.com/openid/authzen
- OpenID Slack: #wg-authzen
- Meeting notes & docs: https://hackmd.io/@oidf-wg-authzen
- Email: omri@aserto.com, david.brossard@axiomatics.com