YAHOO! JAPAN

Athenz + SPIFFE によるアクセス制御

ヤフー株式会社

矢野 達也

2019/05/14

自己紹介

矢野 達也

Web ServiceやSmartphone Appの開発/運用に従事した後、現在はAthenzのDevOpsを行うチームでProduct Ownerを担当しています。

Athenz OSSのContributorとしても活動しており、社外での活動も行なっています。

今やっていること

Athenz の Yahoo!JAPAN 社内での導入、機能拡充など

好きなもの

自動化、システム連携など

アジェンダ

1. SPIFFE standards

2. Athenz による X.509証明書の自動配布

3. Athenz による Fine-grained Authorization

4. Athenz with SPIFFE ID

SPIFFE standards

SVID and SPIFFE ID

- SVID
  - X.509-SVID 
  - JWT-SVID
- SPIFFE ID
  - サービスを直接識別 (Identifying services directly) 
  - サービスとそのオーナーを識別 (Identifying service owners) 
  - 不透明（外部依存）な識別子 (Opaque SPIFFE identity)

SPIFFE ID

- サービスを直接識別 (Identifying services directly) 

  spiffe://staging.example.com/payments/web-fe

  spiffe://staging.example.com/payments/mysql

- サービスとそのオーナーを識別 (Identifying service owners) 

  spiffe://k8s-west.example.com/ns/staging/sa/default

- 不透明（外部依存）な識別子 (Opaque SPIFFE identity)

  spiffe://example.com/9eebccd2-12bf-40a6-b262-65fe0487d453

Workload API

- SVID を各 Workload に配布するための仕組み
- Zero Trust Network では、 SVID を配布するために Workload をどのように認証するかが課題
- Athenz では Copper Argos という検証の仕組みを提供

AthenzによるX.509証明書の自動配布

ATHENZ とは

- クラウド環境でのシステム間アクセス制御
- ロールベースのアクセス制御（RBAC）
- Yahoo Inc.（現 Verizon Media）が開発しオープンソース化

Athenzの機能

- Service Authentication
  - 各 Workload に X.509証明書 を自動配布 (Copper Argos)
- Authorization
  - Roleベースのアクセス制御 (RBAC)
  - Policy による Fine-grained Authorization

AthenzによるX.509証明書の自動配布 (Copper Argos)

- 各 Workload に X.509証明書 を自動配布する仕組みを提供
  - Workload をどのように認証するかはクラウド環境毎に異なる

Cloud computing environments

OpenStack

Kubernetes

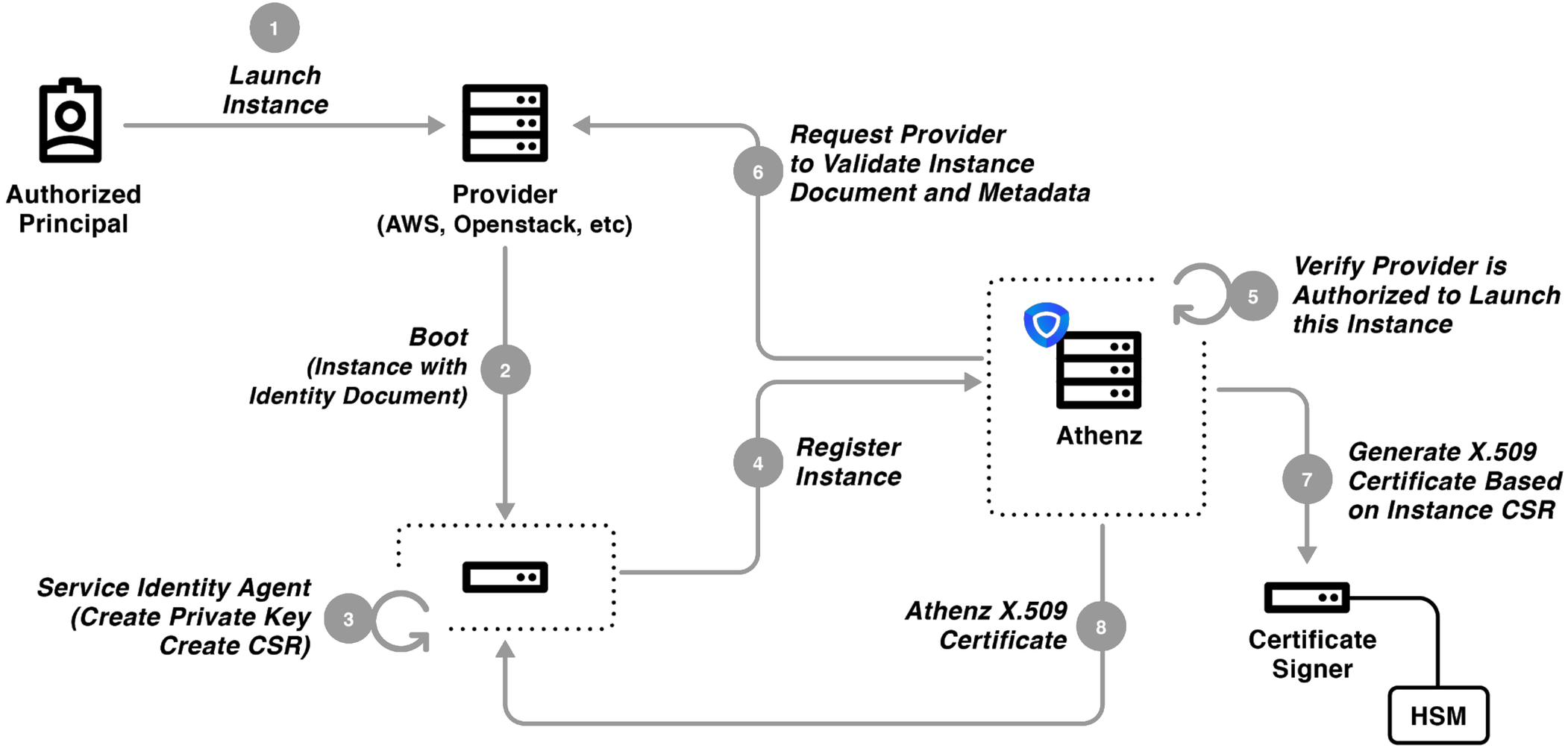
Screwdriver

Amazon EC2

AWS ECS

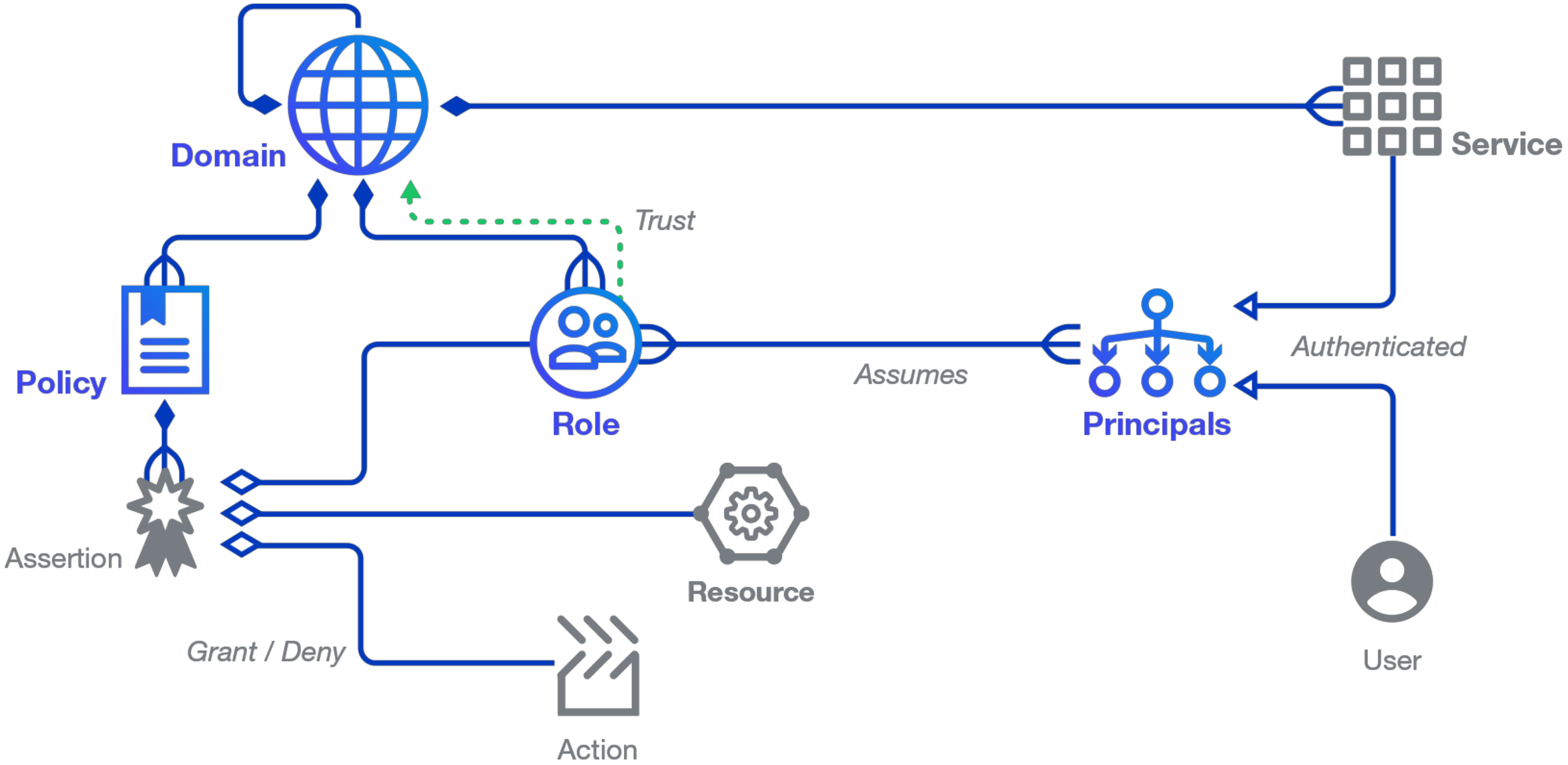
AWS Lambda

Copper Argos

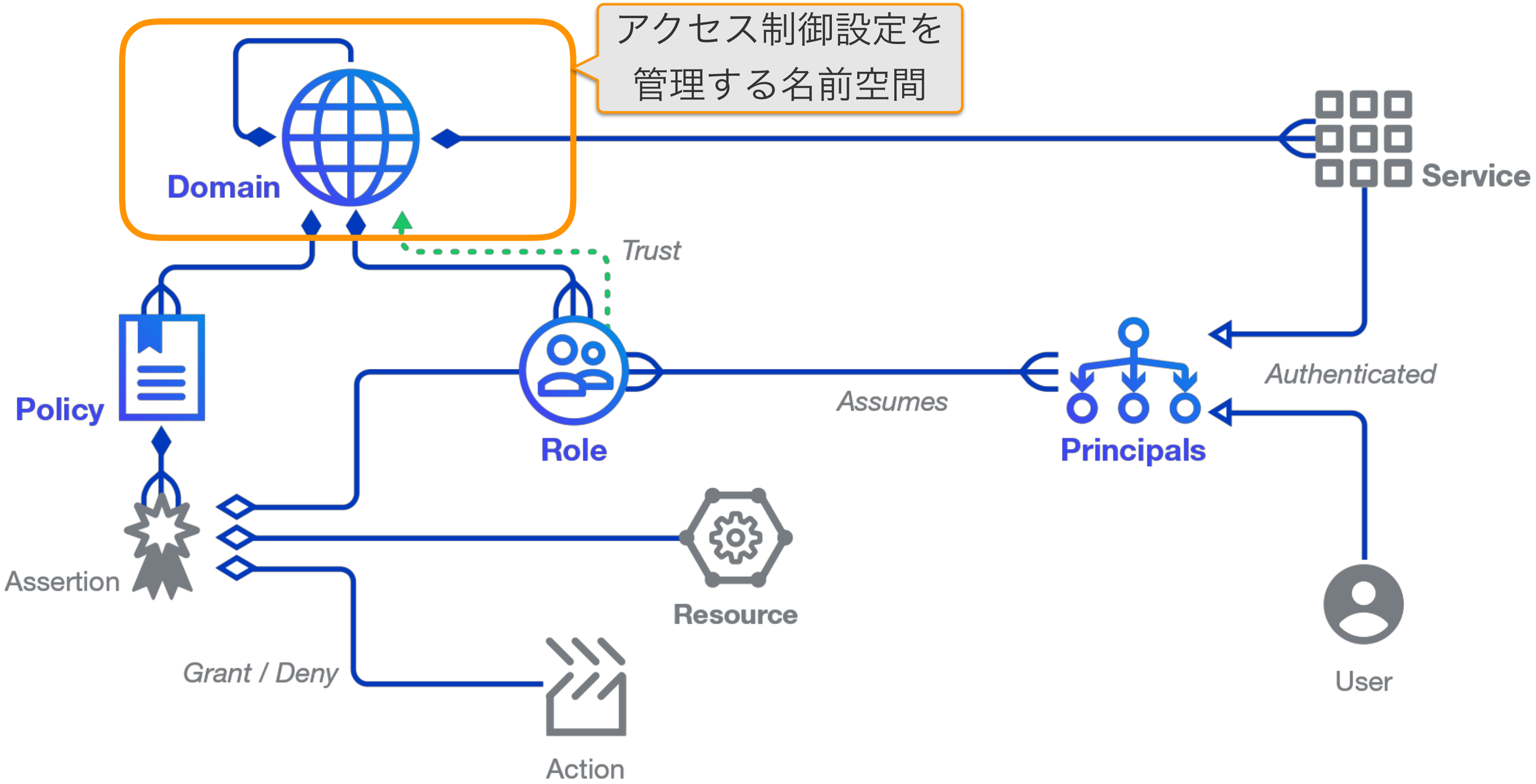


Athenz による Fine-grained Authorization

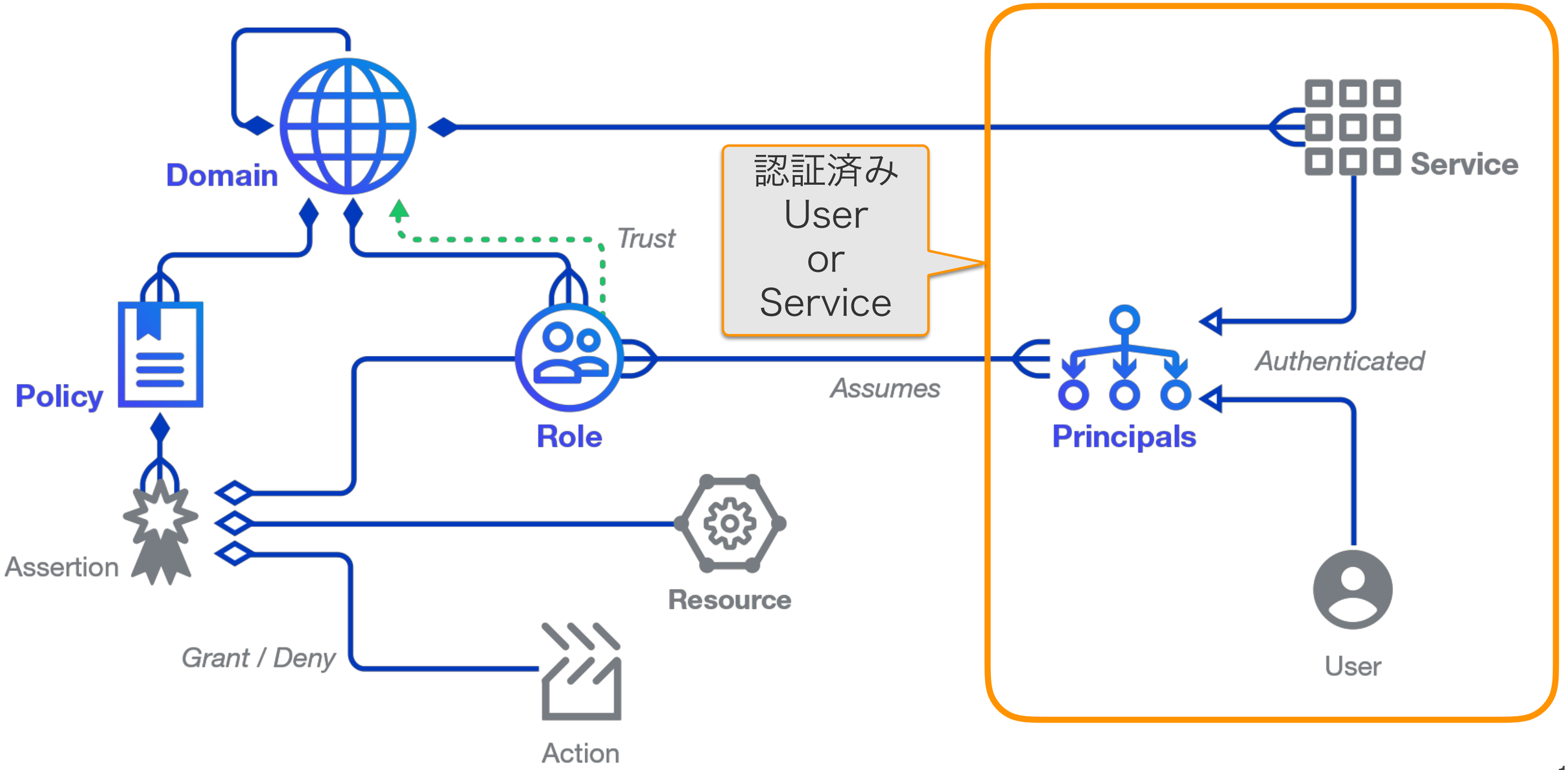
Athenz Data Model



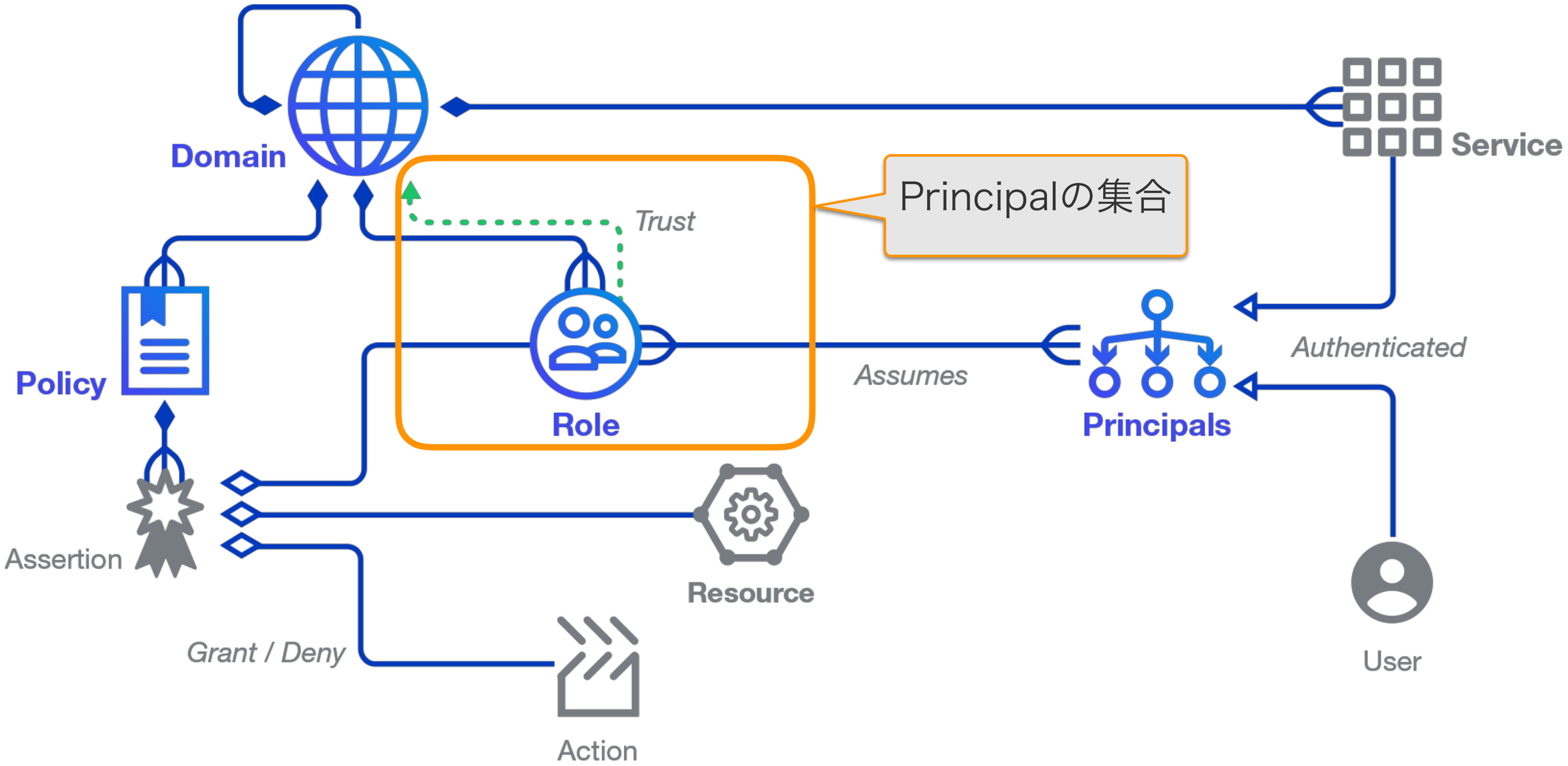
Domain



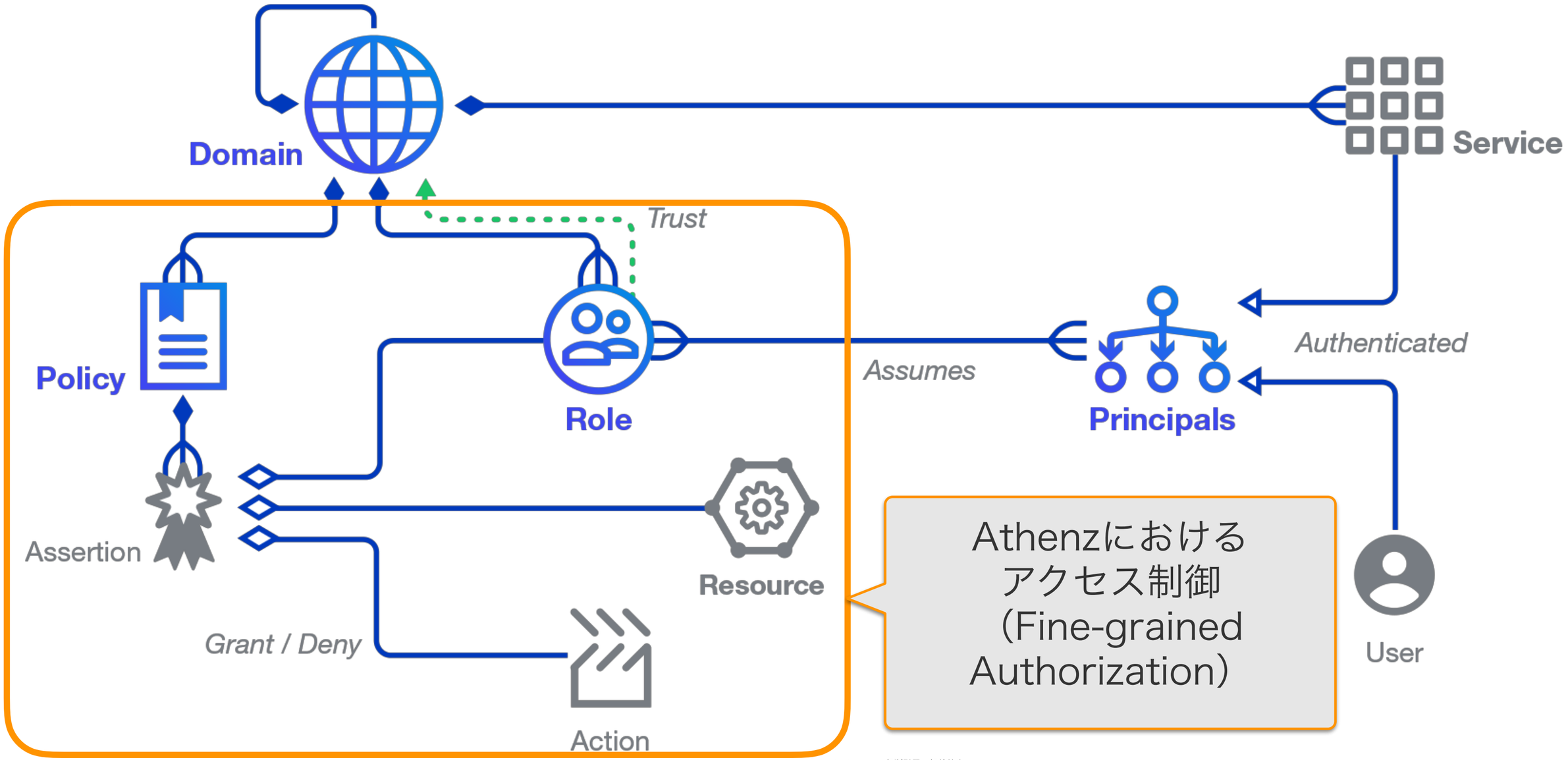
Principal



Role

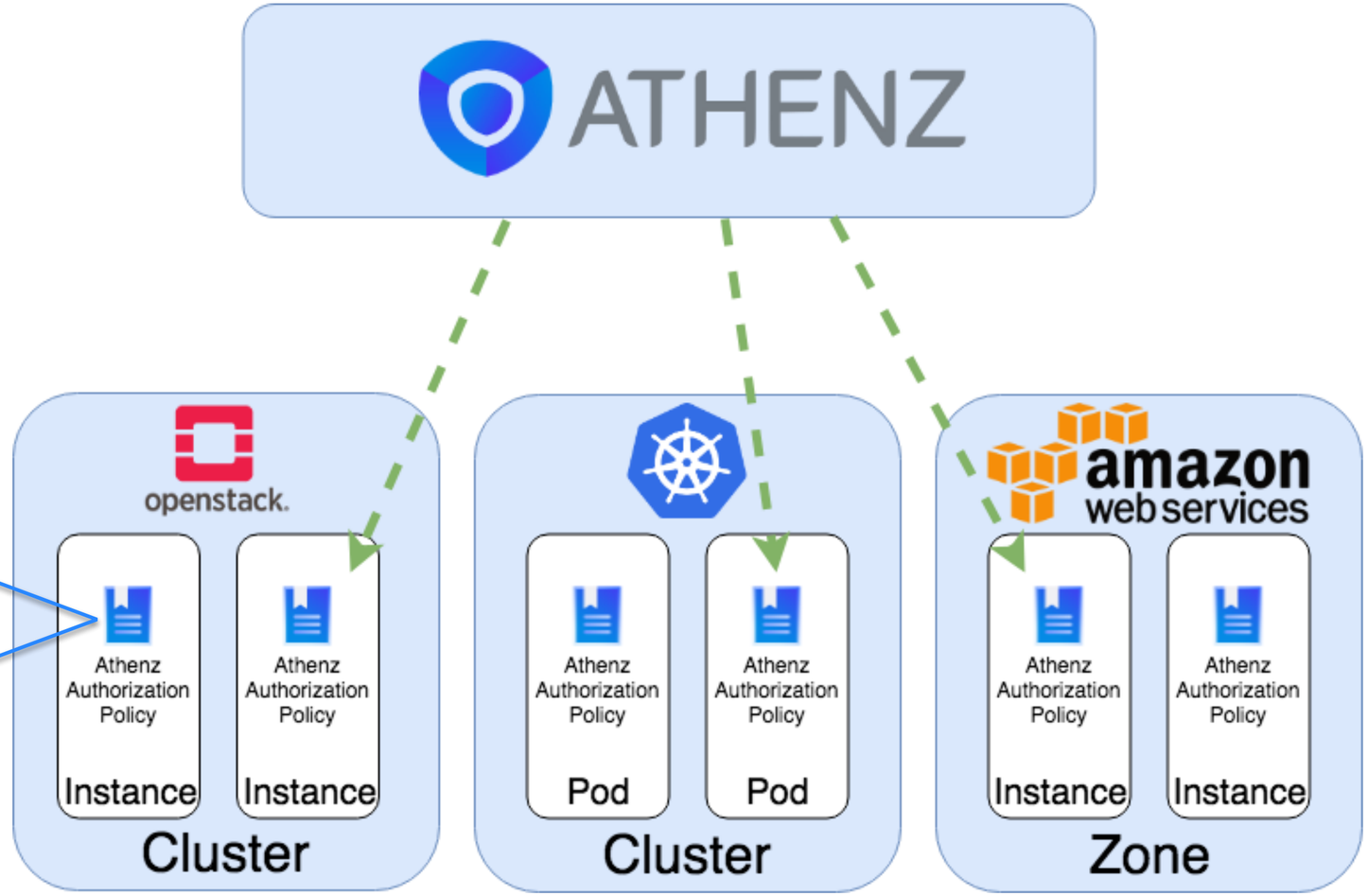


Policy (Fine-grained Authorization)

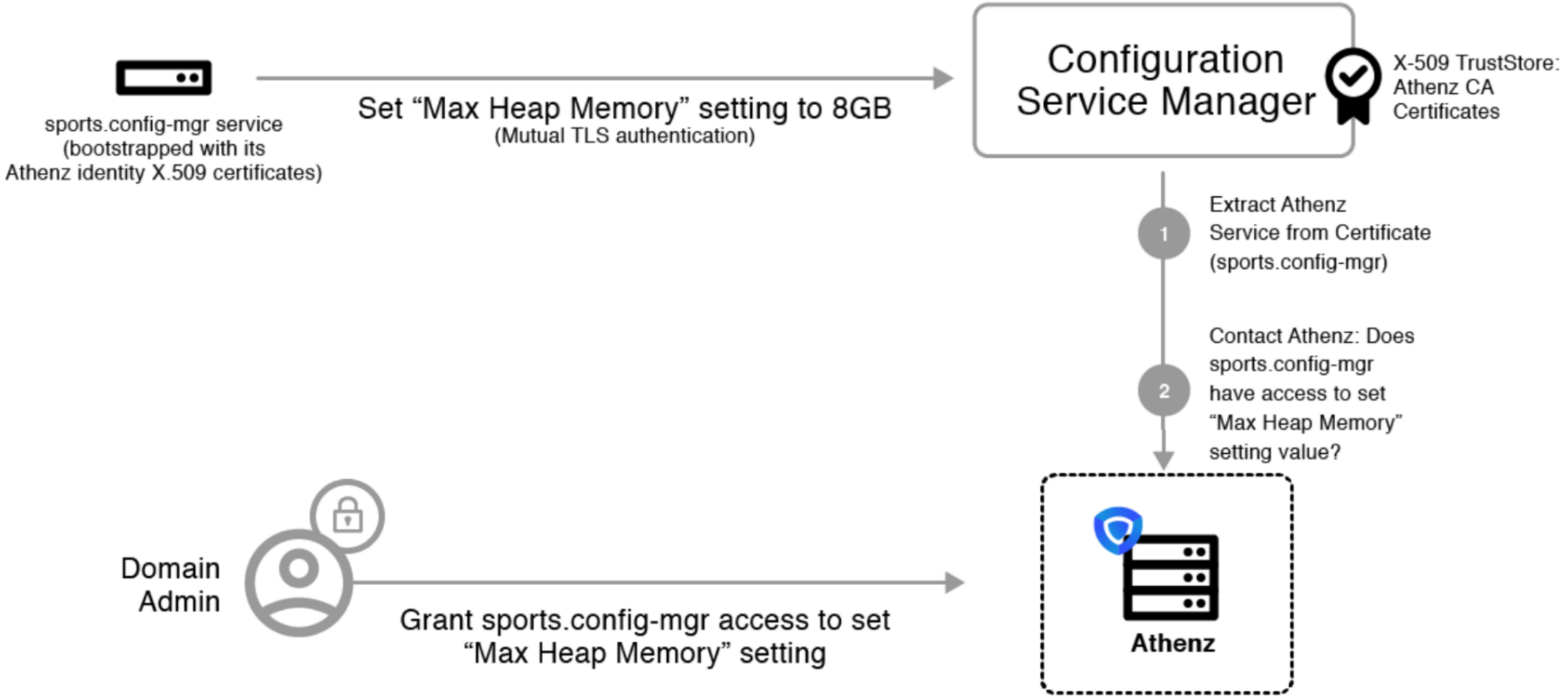


Athenz による Single Source of Truth

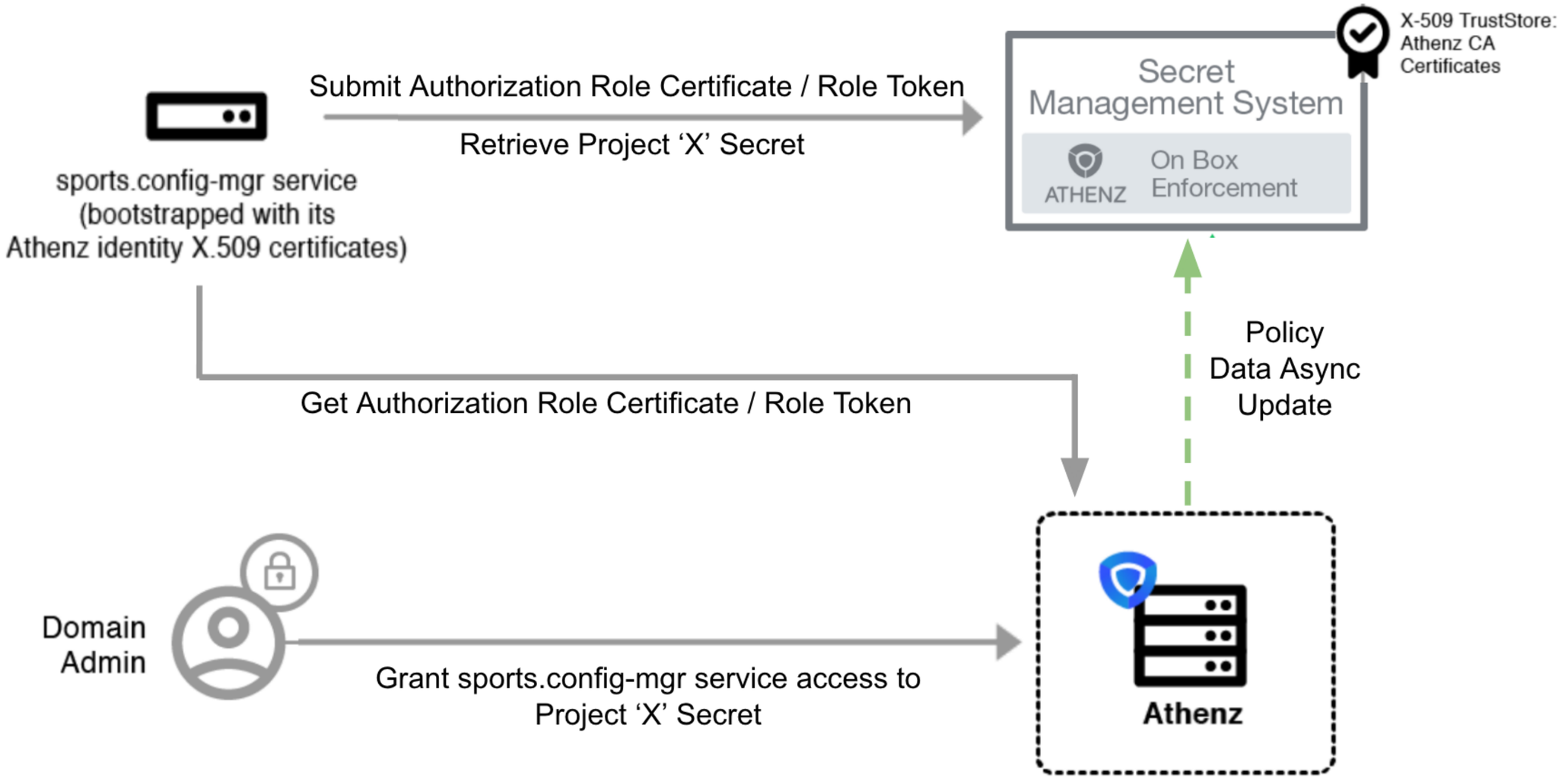
```yaml
domain:
    name: athenz
    audit_enabled: false
    modified: 2018-12-11T08:21:25.896Z
    roles:
        - name: admin
          members:
            - user.admin
        - name: frontend
          members:
            - athenz.instance
    policies:
        - name: admin
          assertions:
            - grant * to admin on *
        - name: blacklist
          assertions:
            - deny post to admin on webapi/secret
        - name: whitelist
          assertions:
            - grant get to frontend on webapi/backend
            - grant post to frontend on webapi/backend
    services:
        - name: athenz.instance
          modified: 2018-12-10T23:45:48.188Z
          publicKeys: []
```



アクセス制御フロー その1：中央アクセス制御



アクセス制御フロー その2：分散アクセス制御



Athenz with SPIFFE ID

SPIFFE ID

- サービスを直接識別 (Identifying services directly) 

  spiffe://<athenz-domain>/sa/<athenz-service>

  spiffe://<athenz-domain>/ra/<athenz-role>

  e.g.) spiffe://sports/sa/config-mgr

- サービスとそのオーナーを識別 (Identifying service owners) 

  spiffe://<provider-cluster>/ns/<athenz-domain>/sa/<athenz-service>

  spiffe://<provider-cluster>/ns/<athenz-domain>/ra/<athenz-role>

  e.g.) spiffe://k8s-west.cluster/ns/sports/sa/config-mgr

今後の展望

- Athenz 自体の Docker/Kubernetes deployment 対応
- Kubernets 向け Copper Argos 用 Sidecar Image

参考情報

Athenz

- Website : http://www.athenz.io
- Github: https://github.com/yahoo/athenz
- Slack Channel: https://athenz.slack.com/
- Discussion Group:
  - Google Group: Athenz-Users
- Questions or Comments:
  - Tatsuya Yano: https://github.com/tatyano

Q & A

Appendix

- Athenz with Istio

https://www.youtube.com/watch?v=jhutgE6NwsM

- Slides

https://github.com/tatyano/SPIFFE-Meetup-Tokyo-1

YAHOO! JAPAN