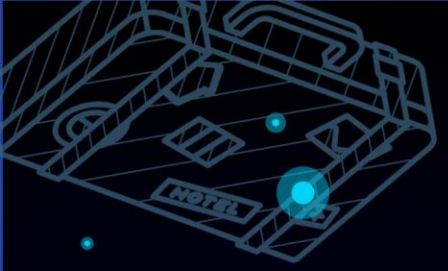
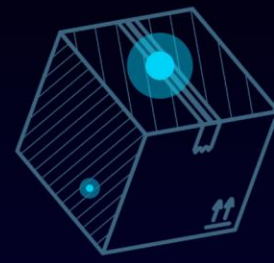
Securing Microservice-based APIs







identiverse

#identiverse

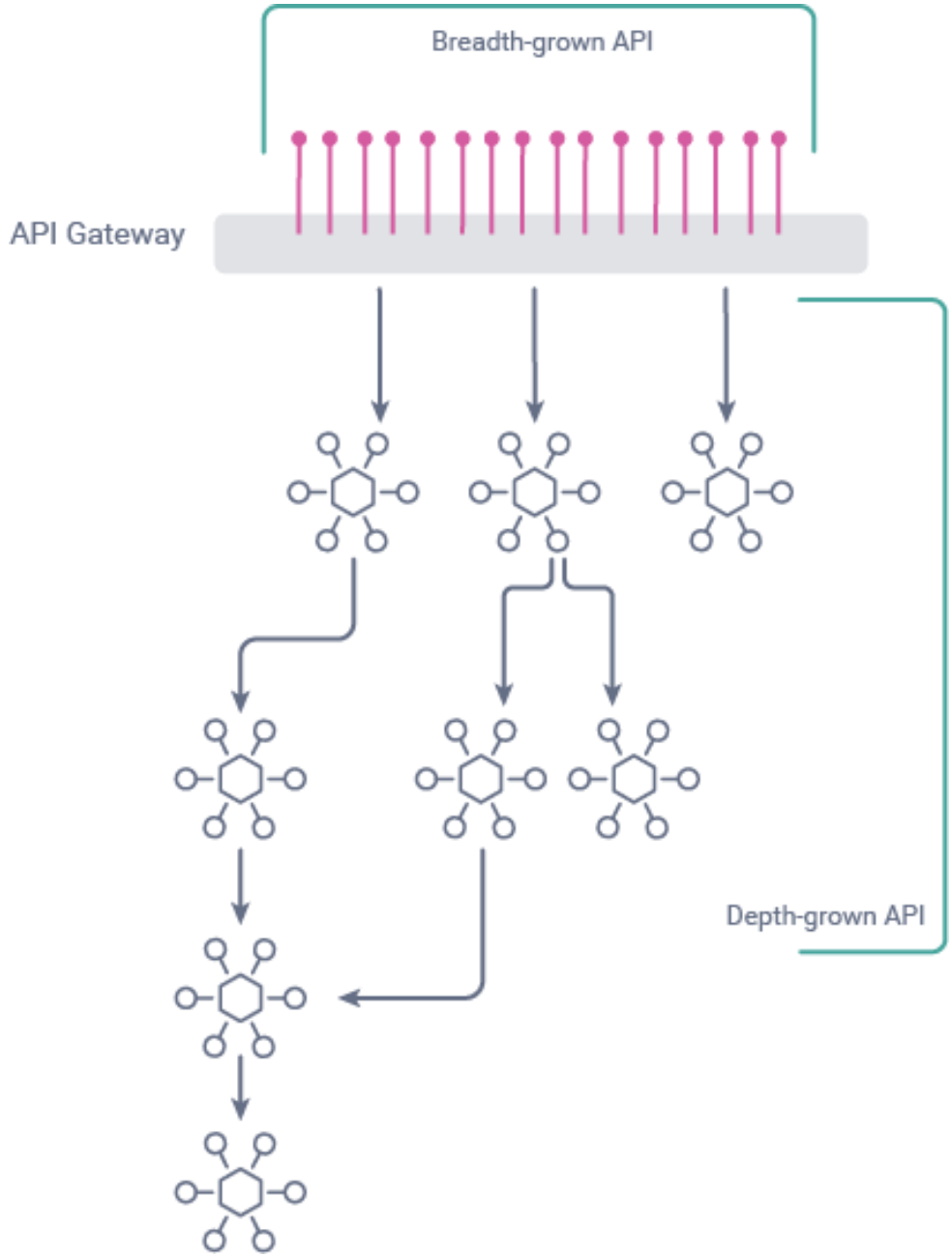
Jonas Iggbom

Director of Sales Engineering

Curity

Agenda

- API Growth – Breath vs. Depth
- Scopes & Claims
- Multi-layered Authorization
- Entitlement Management System


Breadth-grown API
API Gateway
Depth-grown API

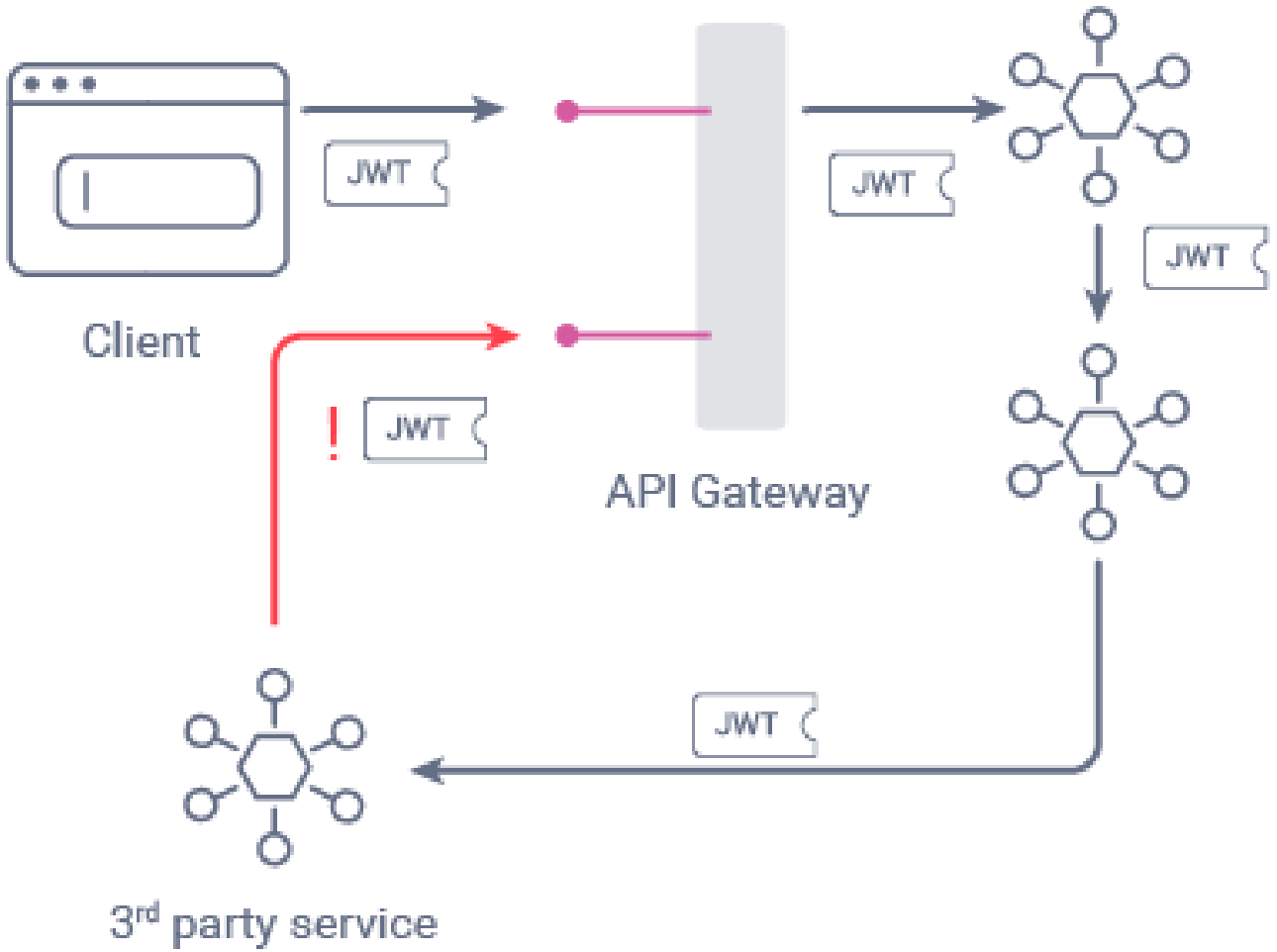
APIs Growing Wide

- Tens or hundreds of endpoints exposed
- Same access token can call any endpoint
- Scopes can help but can lead to scope explosion

APIs Growing Deep

- Call to one endpoint invokes multiple subsequent API calls

- Dangerous if downstream service is an external 3rd party


JWT
JWT
JWT
Client
!
JWT
API Gateway
JWT
3rd party service

Tokens

- Transport attributes needed to perform authorization.
- Tokens are issued differently. Depends on client used to request a token and scopes requested.
- Tokens bound to a specific application, API or use case.

Claims

- Claims are assertions allowing an application or API to trust the attributes.
  - “Curity asserts that Alice is a teller in California”
- Claims allows the user to consent what information or data that it shares with an app or API.

Claims-based Authorization

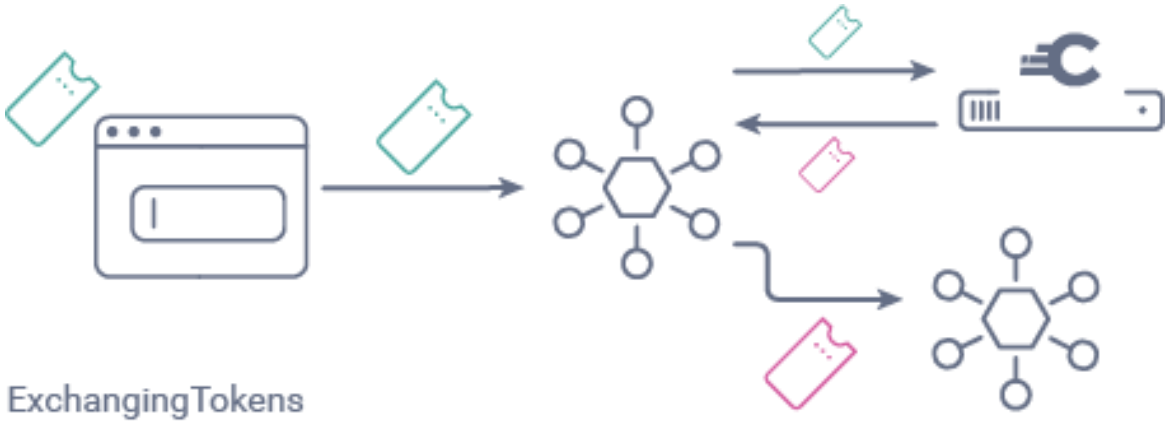
- Audience (“aud”) claim
- Custom claims
- API to check where request is coming from to prevent deep access.

Token - example

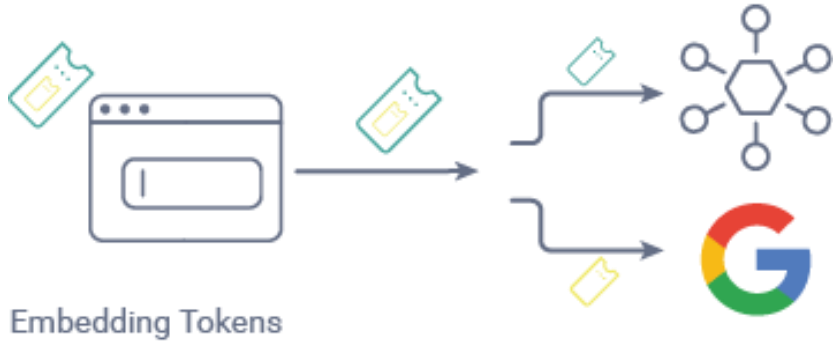
```
{
    sub d160e26d96888f1cac5b5ba8191df77d4053101551d172017413d85b36caa978
    purpose access_token
    iss https://idsvr.example.com/oauth/v2/oauth-anonymous
    token_type bearer
    client_id www
    aud www
    scope read_order
    role teller
    region California
    exp 1641837808
    ...
}
```

Token-Sharing

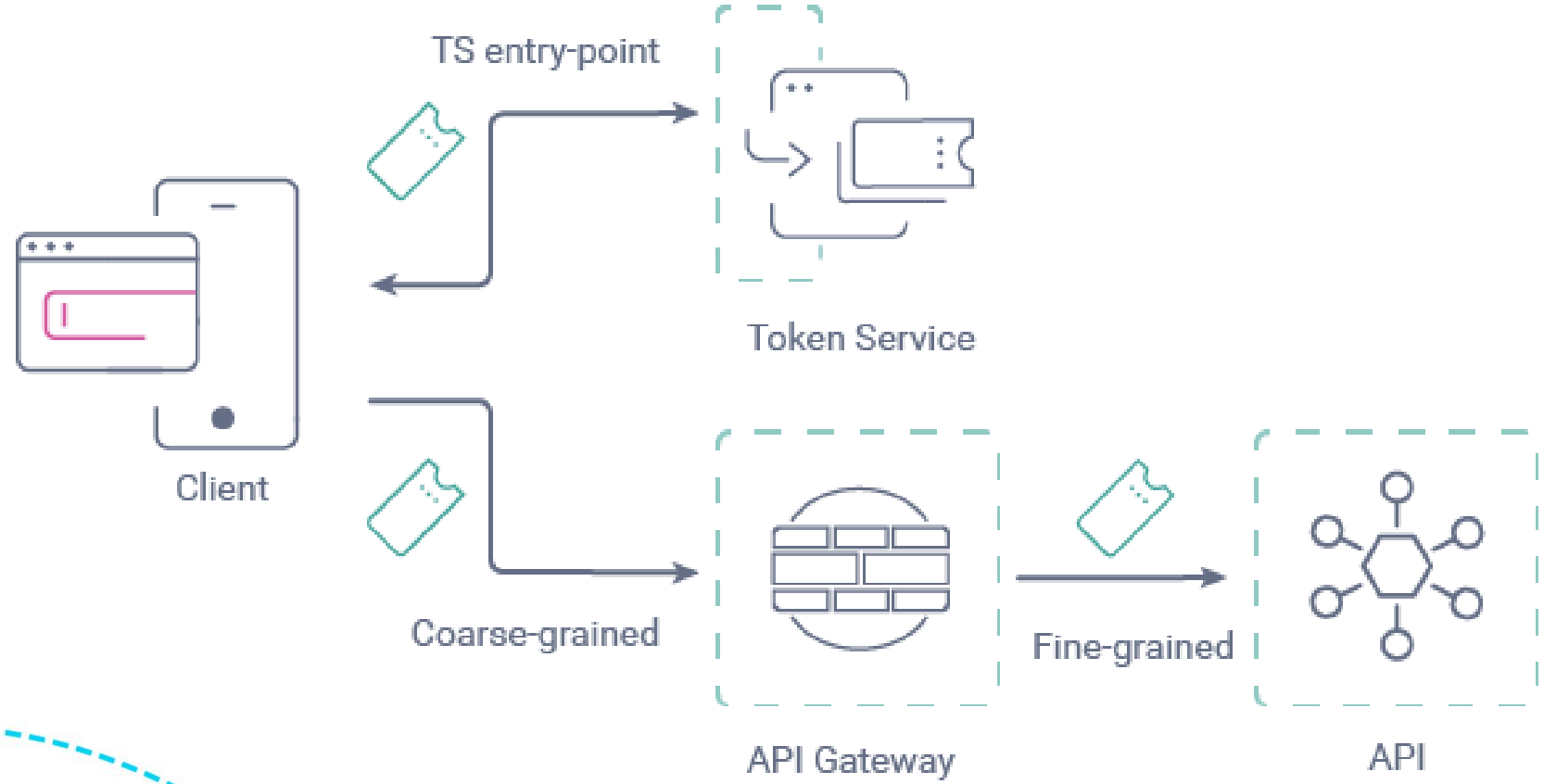
- Different approaches but typically
  - Token Exchange (RFC 8693)
  - Embedded Access Token



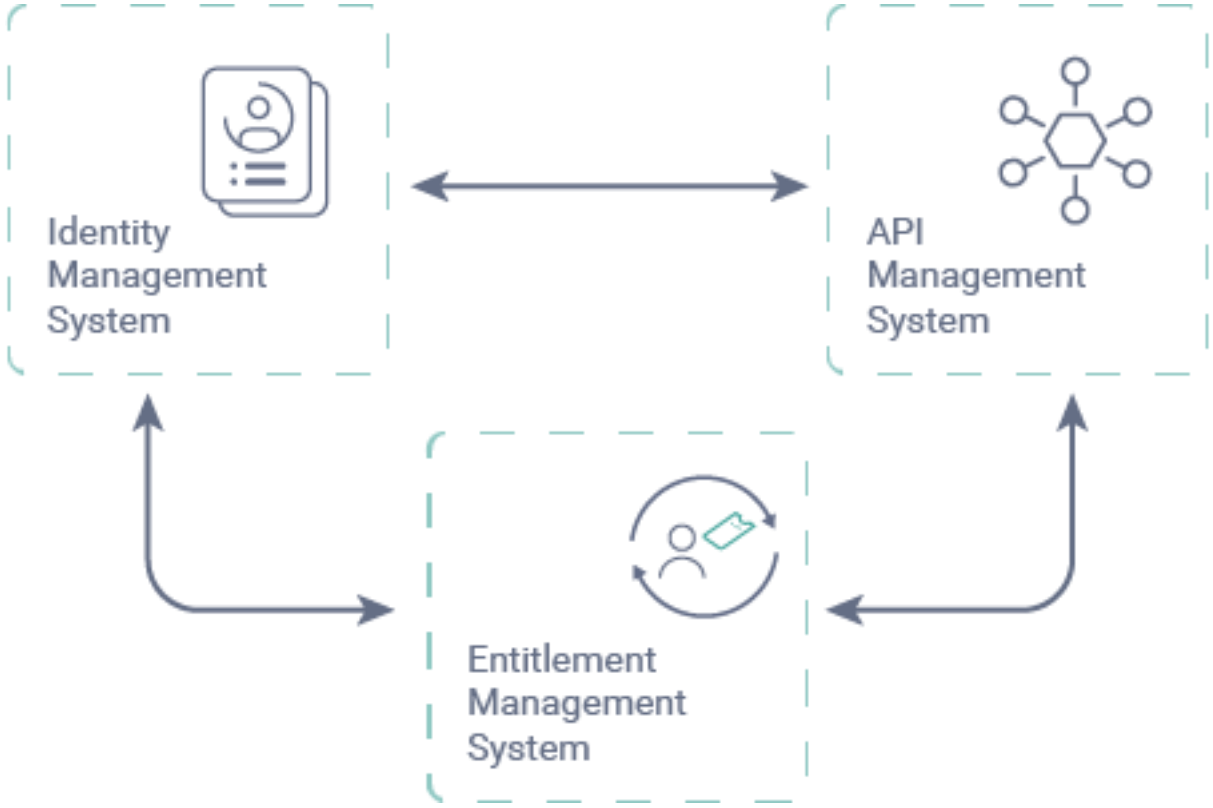
- Limits the actions the downstream service can perform.



Multi-Layered Authorization



The Entitlement Management System

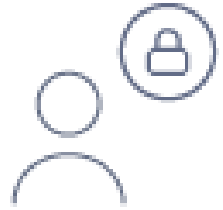


The Entitlement Management System

Policy
Administration
Point

Policy
Decision
Point

Policy
Information
Point

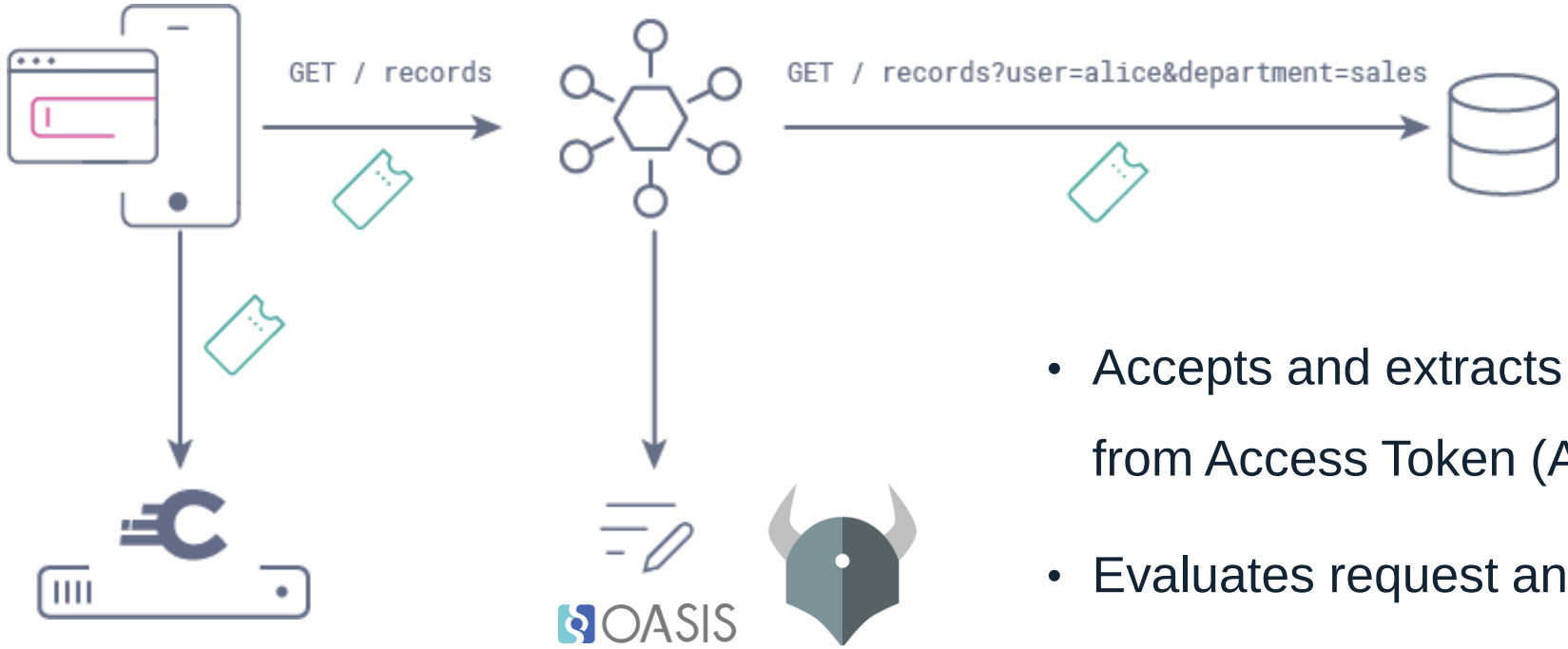


Policy
Enforcement
Point

OPA

XACML 3.0

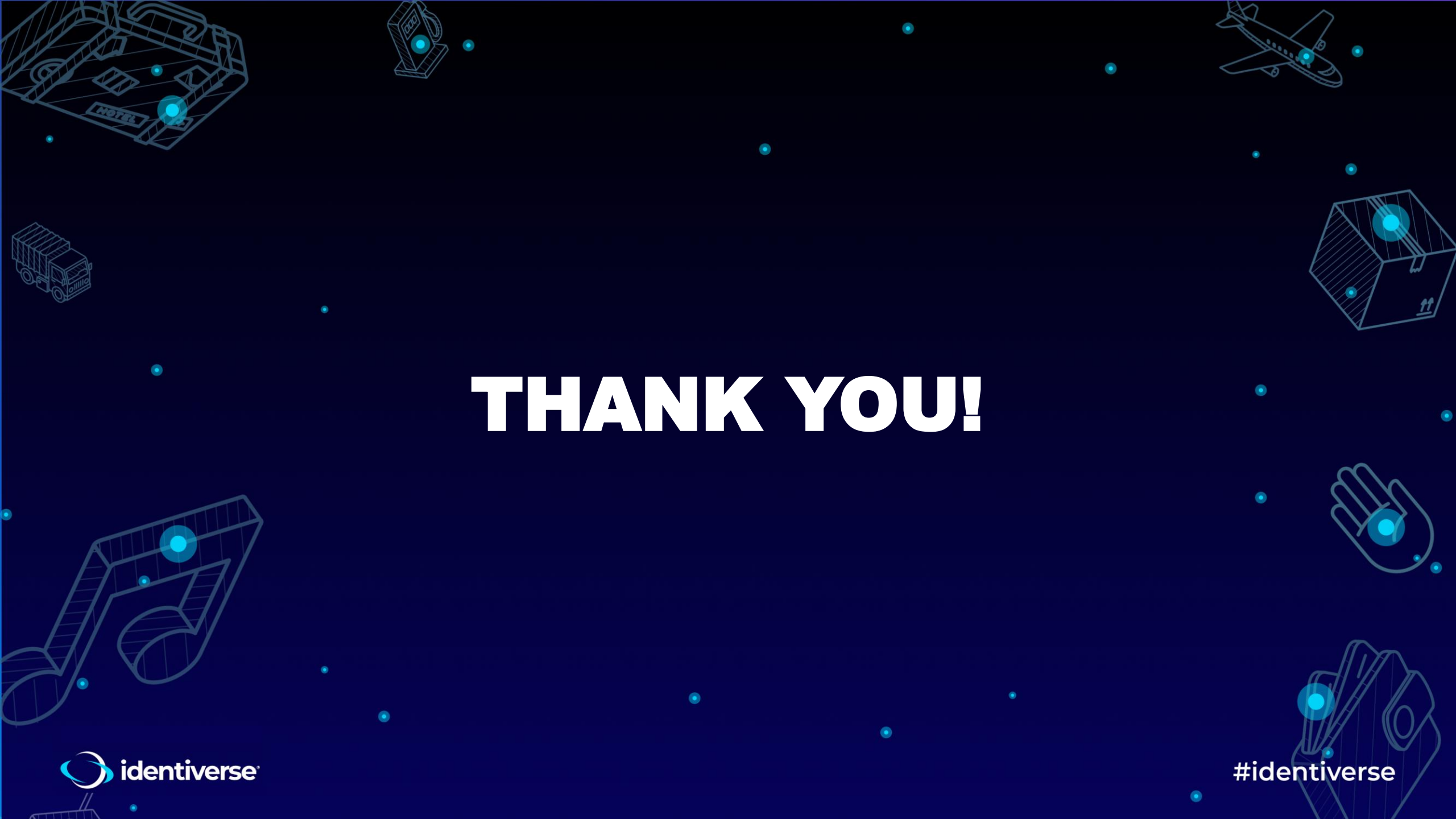
The Entitlement Management System



- Accepts and extracts relevant information from Access Token (AT)
- Evaluates request and AT against policy
- Access decision returned

Conclusion

- Leverage the ”aud” claim and other claims in the token to determine what endpoints can be accessed
- Use token sharing approaches to prevent token reuse in deep APIs
- Multi-layered authorization leveraging an EMS


THANK YOU!
identiverse
#identiverse