Identity Chaining

Rifaat Shekh-Yusef, Pieter Kasselman
OAuth WG, IETF116, Yokohama, Japan
March 31, 2023
Collaborators

- **Arndt Schwenkschuster**, Software Engineer, Microsoft
- **Atul Tulshibagwale**, CTO, SGNL
- **George Fletcher**, Executive Distinguished Engineer – Identity Architect, CapitalOne
- **Hannes Tschofenig**, Chair OAuth WG @ IETF
- **Joe Jubinski**, Chief Architect for Cloud Integration & Interop
- **Kelley W Burgin**, Cybersecurity Engineer, The MITRE Corporation
- **Michael Jenkins**, Secure Protocol Standards Lead, NSA-CCSS
- **Pieter Kasselman**, Identity Standards Architect, Microsoft
- **Rifaat Shekh-Yusef**, IAM Director @ EY, Chair OAuth WG @ IETF
Goal

Enable services within the **same trust boundary** and **across trust boundaries** to securely and interoperably convey **identity, authentication, call chain, and call context information** in communication between **independent** services for authorization and audit purposes.
Motivation

- Securing authorization and identity information in micro-service communication
- Defense against microservice attacks
  - Prevent the access of arbitrary data to/from other microservices.
- Needs open-standard to work across multiple cloud platforms and hybrid deployments.
Identity and AuthZ Information

- Preserve Identity of the initiating principal
- Service identity of the calling service
- Service identities of participants in the call chain
- Authorization scope defined by the caller
- Authorization scope defined previously called services in the call chain
- Argument context defined by the initiating principal
- Argument context defined anywhere in the call chain
Background

- **Prior Work**
  - Netflix blog - Edge Authentication, protobuf “Passport” token, HMAC signatures
  - Athenz - Verizon supported open-source for “AuthNZ”; Centralized and decentralized authz

- **Related presentations**
  - George Fletcher at Identiverse 2020 - short-lived Transaction Tokens, JWT based
  - Dr. Kelley W. Burgin at IETF 114 - OAuth token chaining
  - Atul Tulshibagwale- Fine Grained Transactional Authorization
  - Rifaat Shekh-Yusef - JWT Embedded Token
Use Cases

- API Security Use Case
- Preserve User Context across Trust Domains
- Report Building in a Federated Environment
Diverse Subjects with Embedded Tokens (1 of 3)

Wrap the token inside another token when crossing trust boundaries.
Different Subjects with Embedded Claims (2 of 3)

Transcribe a subset of claims when crossing trust boundaries.
Allow different identifiers to be used in different domains.
Questions?