draft-liu-oauth-a2a-profile

Chunchi Peter Liu， Yuan Ni

IETF 125, Shenzhen

Transaction Token Profiles for A2A Calls

What:

- Transaction Tokens (*draft-ietf-oauth-transaction-tokens-08*) are designed to maintain and propagate **user & workload identity, authorization context** throughout the service call chain.

- We Extend this mechanism from service-to-service to **Agent-to-Agent** scenarios, enabling secure propagation of
  - **User & Agent Identity**
  - **Authorization Context**
  - **A2A Context**

Transaction Token Profiles for A2A Calls

Why:

- According to *OWASP TOP 10 for Agentic AI Applications*, workflow across multiple agents in facing the risks of **goal hijack, context poisoning, and privilege abuse**.

- Transaction Tokens is a powerful way to solve this by
  - **Preserving the user identity and authorization context**
    -> avoid any deviation from the original user’ s intent
  - **Ensuring decreased scope**
    -> prevent privilege abuse
  - **Utilizing short-lived, task-triggered tokens**
    ->limit replay and lateral use
  - **Preserving the A2A context**
    ->prevent context poisoning and context rot

Transaction Token Profiles for A2A Calls

How:

- Encapsulate **A2A message structures** into Transaction Token claims.

- **scope(purp)**: the immutable purpose of this particular transaction

  ⟵ **Purpose of a specific task:**
  A2A message. task_id

- **tctx:** the details that remain immutable through the call chain

  ⟵ **User input:**
  Inherited from external access token' s authorization details(OAuth 2.0 RAR)

- **rctx**: changeable environmental context of the requested transaction, MAY include any values the TTS determines are relevant to downstream services

  ⟵ **Agent thinking, Status Updates:**
  - A2A message. context_id
  - A2A message. message_id
  - A2A message. role
  - A2A message. metadata

- **Should *scope* derive from *A2A message. task_id* or *scope* from the external access token?**
- **Should we introduce a new claim to carry the A2A context, or directly use the existing *rctx* ?**
- **NOTE: Discussed with author of *draft-oauth-transaction-tokens-for-agents*; potential merger later.**