

Transaction Token Profiles for A2A Calls

Chunchi Peter Liu(liuchunchi@huawei.com)

Yuan Ni(niyuan1@huawei.com)

Yuan Zhou(zhouyuan89@huawei.com)

IETF 125, Shenzhen

Transaction Token Profiles for A2A Calls

Background

Transaction Tokens(*draft-ietf-oauth-transaction-tokens-08*) securely propagate **user identity** and **authorization context** across workloads.

What

- **purp(scope)**
- **rctx**

Transaction Token defined several **immutable** and **changeable** data fields.

We use these **data fields** to protect A2A message from threats like **context manipulation attack** and **context rot**.

Why

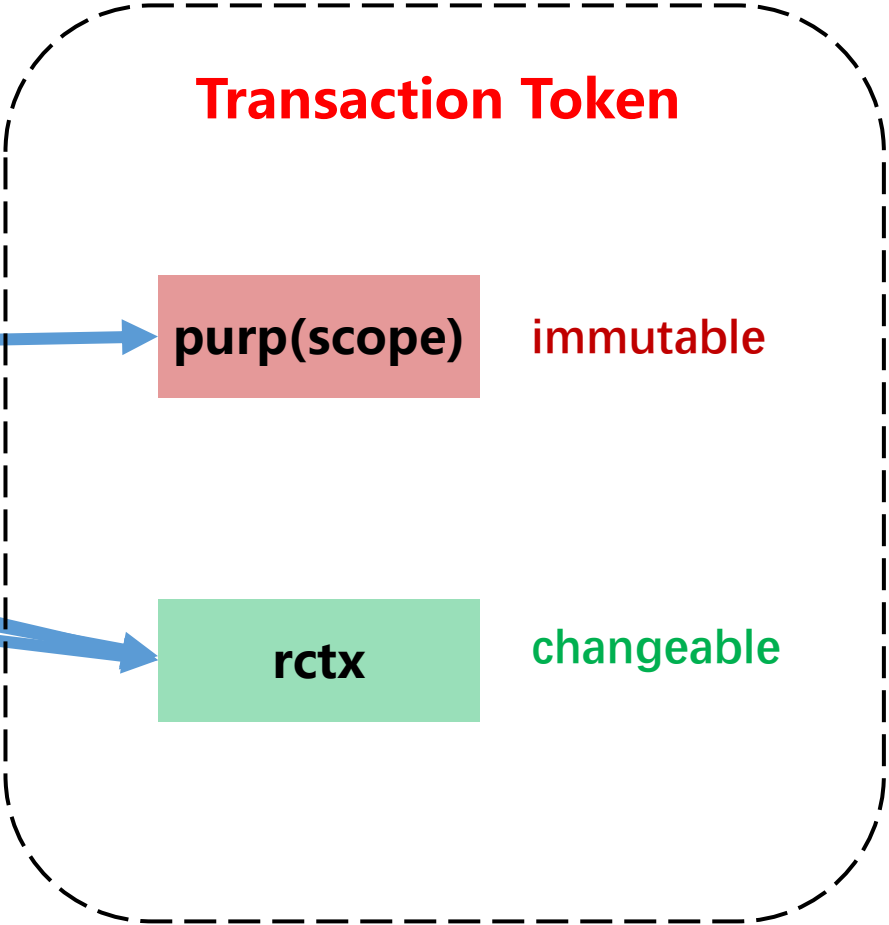
Critical contexts, user intents and **identity** should be **preserved** throughout the entire agent-to-agent call chain..

Draft: <https://www.ietf.org/archive/id/draft-liu-oauth-a2a-profile-00.html>

Transaction Token Profiles for A2A Calls

A2A Message

HTTP HEADER	POST /api/order HTTP/1.1 Content-Type:application/json Authorization: Bearer <Access_Token>
HTTP PAYLOAD	<pre>{ "jsonrpc": "2.0", "method": "message:send", "params": { "message": { "task_id": 1, "context_id": "a7cc0bef..." , "message_id": "296eafce9 " , "role": "ROLE_USER", "parts": [{ "text": "How much is the exchange rate?" }], }, }, }</pre>



@Ashay Raut from AWS suggested creating a new data field *agentic_ctx*

Transaction Token Profiles for A2A Calls

INPUT

```
curl -v -X POST "http://localhost:30000/api/order" \  
-H "Content-Type: application/json" \  
-H "role: ROLE_AGENT" \  
-H "context_id: ctx-shark-001" \  
-H "message_id: msg-uuid-999" \  
-H "task_id: task-abc-123" \  
-H "Cookie: session_id=eyJhbGciOiJSUzI1NiIsImtpZCI6IjJkODU5MzJmImJyZDMxYTlmNmFmMWZhMiwiaWF0IjoxNzczMzY2MTk5LCJhdF9oYXNoIjoiYUpScmZ4VXBqUE9kwlplTTdsZ2NqdyIsImNfaGFzaCI6ImV4XRfAAjwr3-akcWZF76eBJEn14uEpQRekPVMYUXjxmwSpdJsrmsbISK9-mEpSw38W67NmSRMxcAlI4Jm2XxuL9iRX_wiQmOnzdK6bOQ69whw5-Tkw5k77wDpquNbs4WMGvU0vhxqtLeL1UZ_aw" \  
-d '{  
  "stockId": 1,  
  "orderType": "Buy",  
  "quantity": 1  
}'
```

```
-H "role: ROLE_AGENT" \  
-H "context_id: ctx-shark-001" \  
-H "message_id: msg-uuid-999" \  
-H "task_id: task-abc-123" \
```

OUTPUT

```
>  
< HTTP/1.1 200 OK  
< Content-Length: 179  
< Content-Type: application/json  
< Date: Fri, 13 Mar 2020 02:19:05 GMT  
< Txn-Token: eyJhbGciOiJSUzI1NiIsImtpZCI6InBteFZXNmWd4VEQYldhSnVScjAzbWc9PSIsInR5cCI6InR4b190b2t1biJ9.eyJhdwQiOiJodHRwczoMzM2ODM0MywiaXNzIjoiaHR0cHM6LyhhbHoBoYXN0b2Nrcy5jb20vdG9ZW5ldGVzIiwicmVycCI6InRhc2stYWJjLTEyMyIsInjdHgiOnsiY29udGV4dDf9pZViIjp7ImZvcmlhdCI6ImVtYWlsIiwiziW1haWwiOiJzaGVybG9ja0BkZRLY3QuY29tIn0sInR4bii6IjYyNDNDNiYwZmLE5NMtNGI3Yi1imJcwLTVjOWUyODQ8mo7sKRwilc4GZ5-I-e28JJtUQHrBEZedsQ7X7aEyzrR0vVcrF0BuwA9LqPAl7iTtT2qmJF_e01HbEHBzhCF3F-gEhJ60WRUae0g1S9spRrO32XGGmzzkm
```

PAYLOAD

```
{
  "aud": "https://alphastocks.com/",
  "azd": {
    "action": "Buy",
    "quantity": 1,
    "stockId": 1
  },
  "exp": 1773368358,
  "iat": 1773368343,
  "iss": "https://alphastocks.com/tokenetes",
  "purp": "task-abc-123",
  "rctx": {
    "context_id": "ctx-shark-001",
    "message_id": "msg-uuid-999",
    "req_ip": "192.168.65.3",
    "role": "ROLE_AGENT"
  },
  "sub": {
    "format": "email",
    "email": "sherlock@detect.com"
  },
  "txn": "6443baff-196a-4b7b-b270-5c9e2847bf2d"
}
```

<https://github.com/Ann20030/Txn-token-A2A> using tokenetes
<https://github.com/tokenetes>

Does it reveal more profound questions?

Threat: A2A is envisioning a more collaborative future, but new agent-oriented attacks are more implicit (in the data payload, e.g. prompt injection) rather than explicit and structural (in the header).

- In Agent-to-Agent communications, what **security contexts** should always be carried and preserved alongside the call-chain, across 2 or more domains?
 - Never stripped off, in the format of structured, mandatorily carried data fields with integrity protection
 - agent_id, task_id, context_id, original_user_input, user_identity, access_model, identity_provider, is_attested ...
 - To provide sufficient security contextual input to the authorization server
- Do we need consistent access control policies (or patterns) across 2 or more domains?

Come to Thursday 11:15-12:15 AI Agent Security Side Meeting @Hunan Room and discuss!

- <https://github.com/liuchunchi/IETF125-AI-Agent-Security-Side-Meeting>
- <https://www.ietf.org/archive/id/draft-liu-oauth-a2a-profile-00.html>