Transaction Tokens for Agents

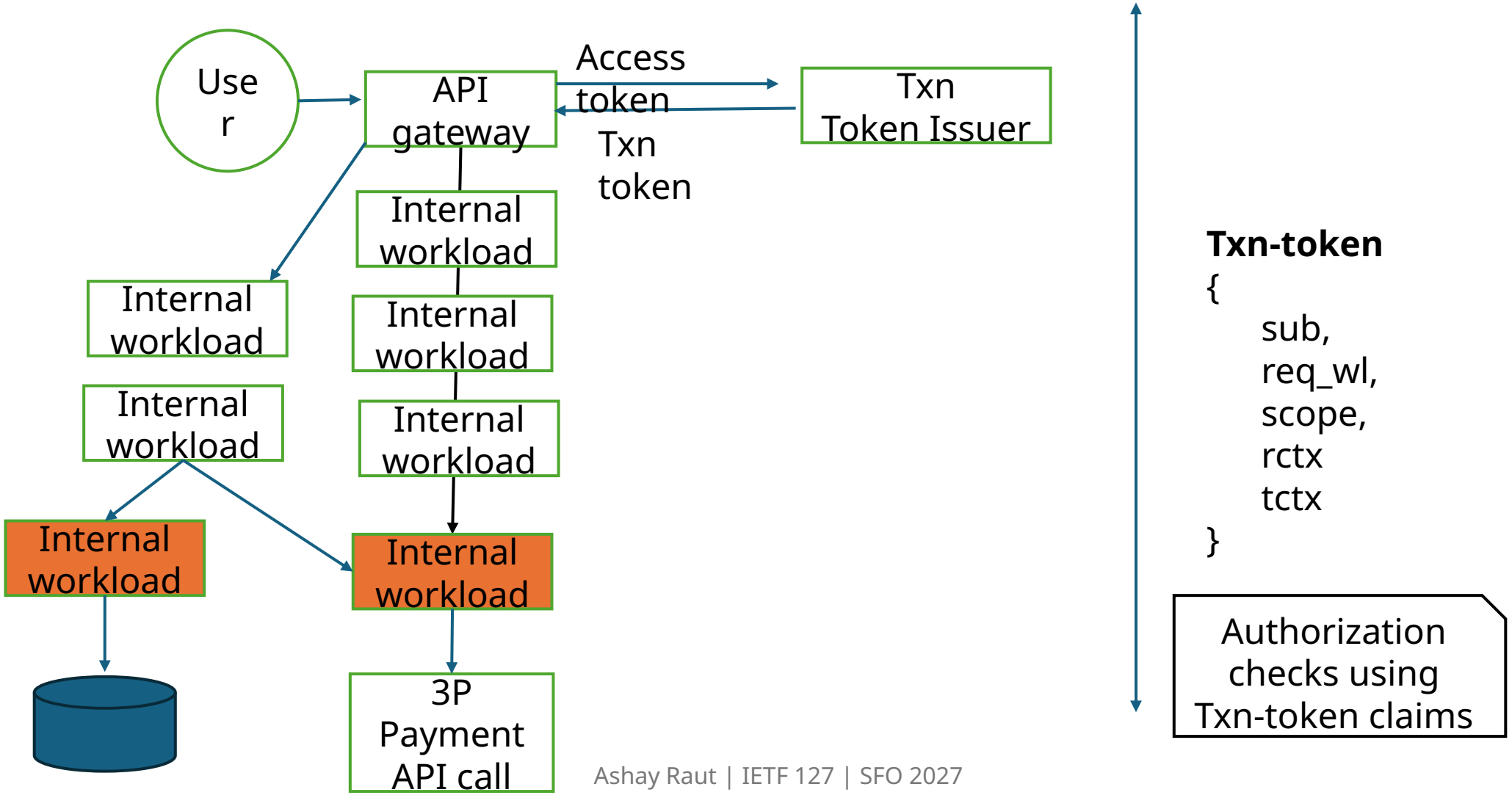
`draft-araut-oauth-transaction-tokens-for-agents-03`

`draft-araut-oauth-transactiontokens-bcp-00`

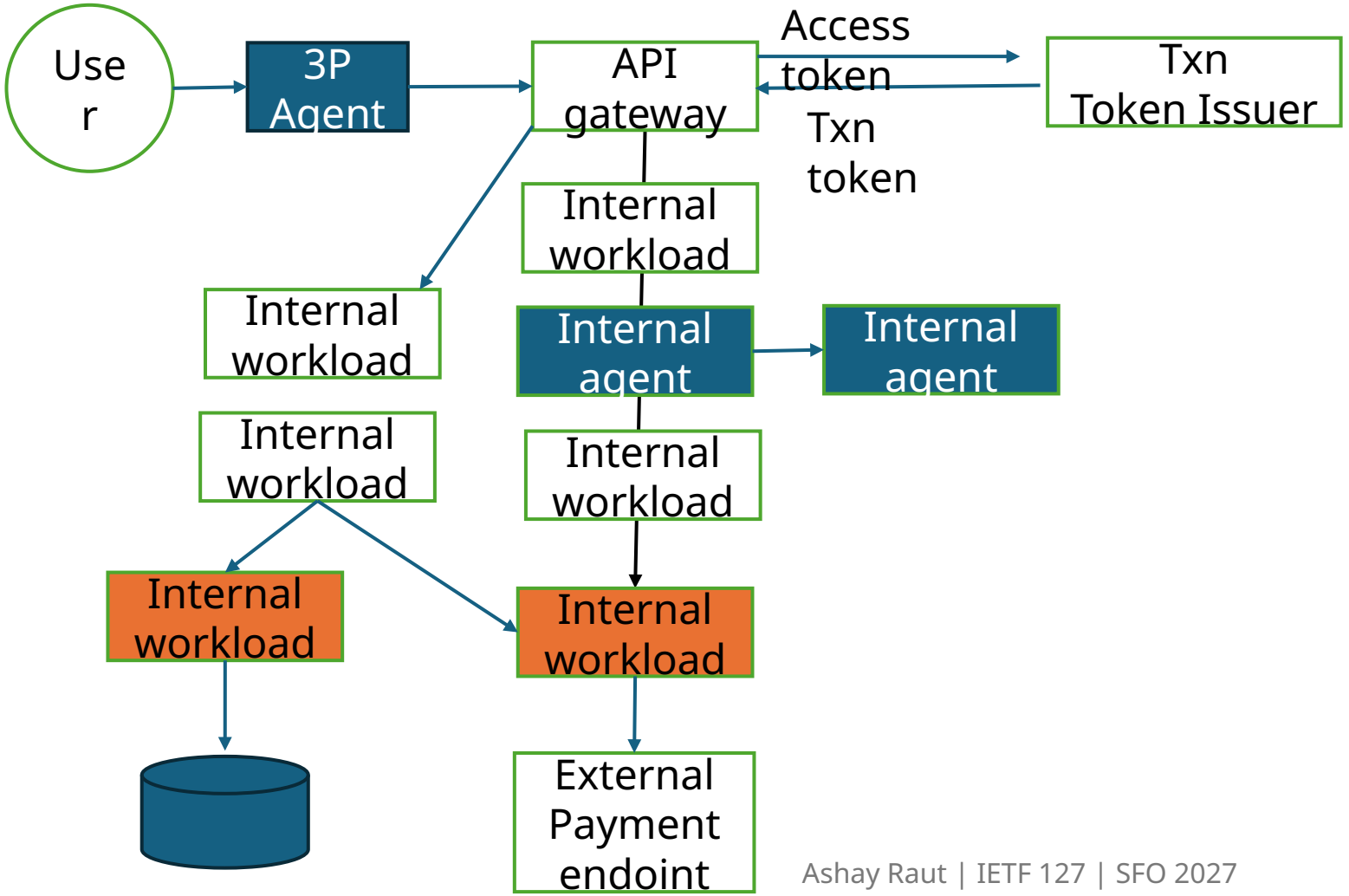
Ashay Raut · Amazon

IETF · San Francisco · November 2026

Transaction Tokens and workloads



Agents and agentic_ctx



Txn-token {
sub,
req_wl,
scope,
rctx
tctx,

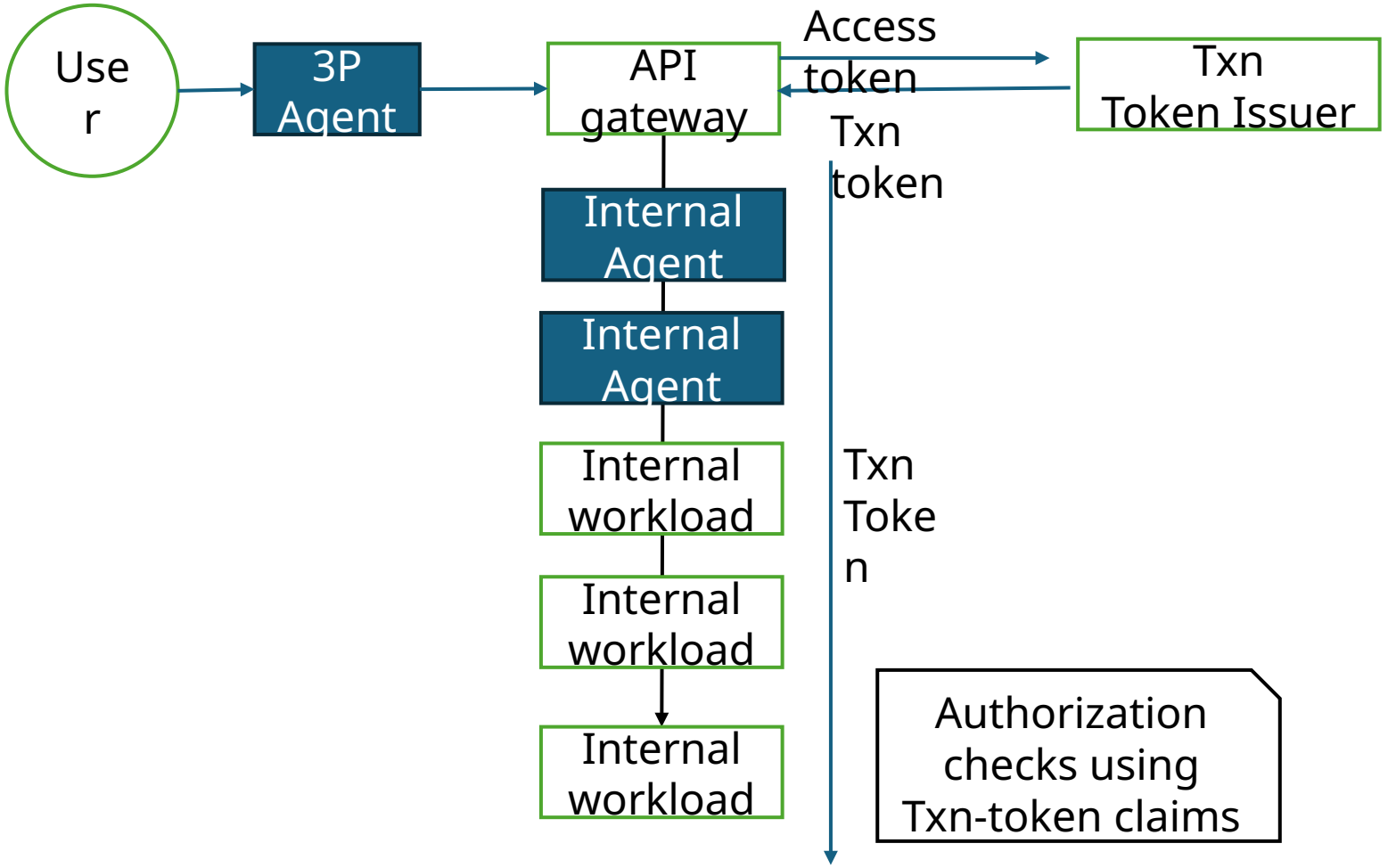
agentic_ctx
}

Authorization checks using Txn-token claims

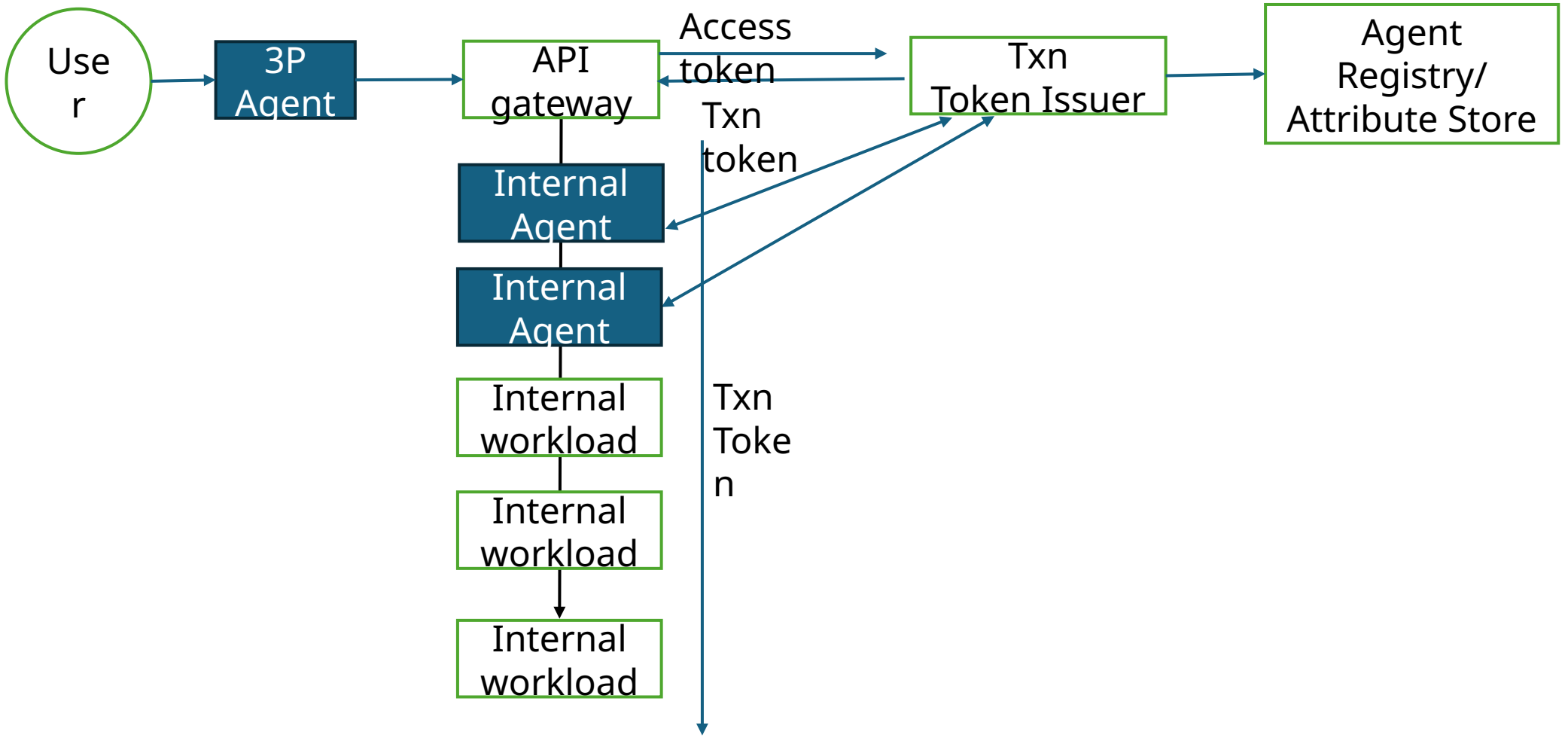
Why?

- 1000s of Agents are already part of our trust domains
- Cryptographic provenance across multi-hop agent call chains
- No audit closer to the data about agent-initiated actions.
- Agents -> Tools -> Fans out to workloads. Call graph changes.
- Workloads closer to the data / critical operations need control
  - Never allow any agent in trust domain to update user account data
  - Allow only agents running in secure environments to access user personal data
  - Allow only internal agents to access sensitive data
  - ...defense in depth checks

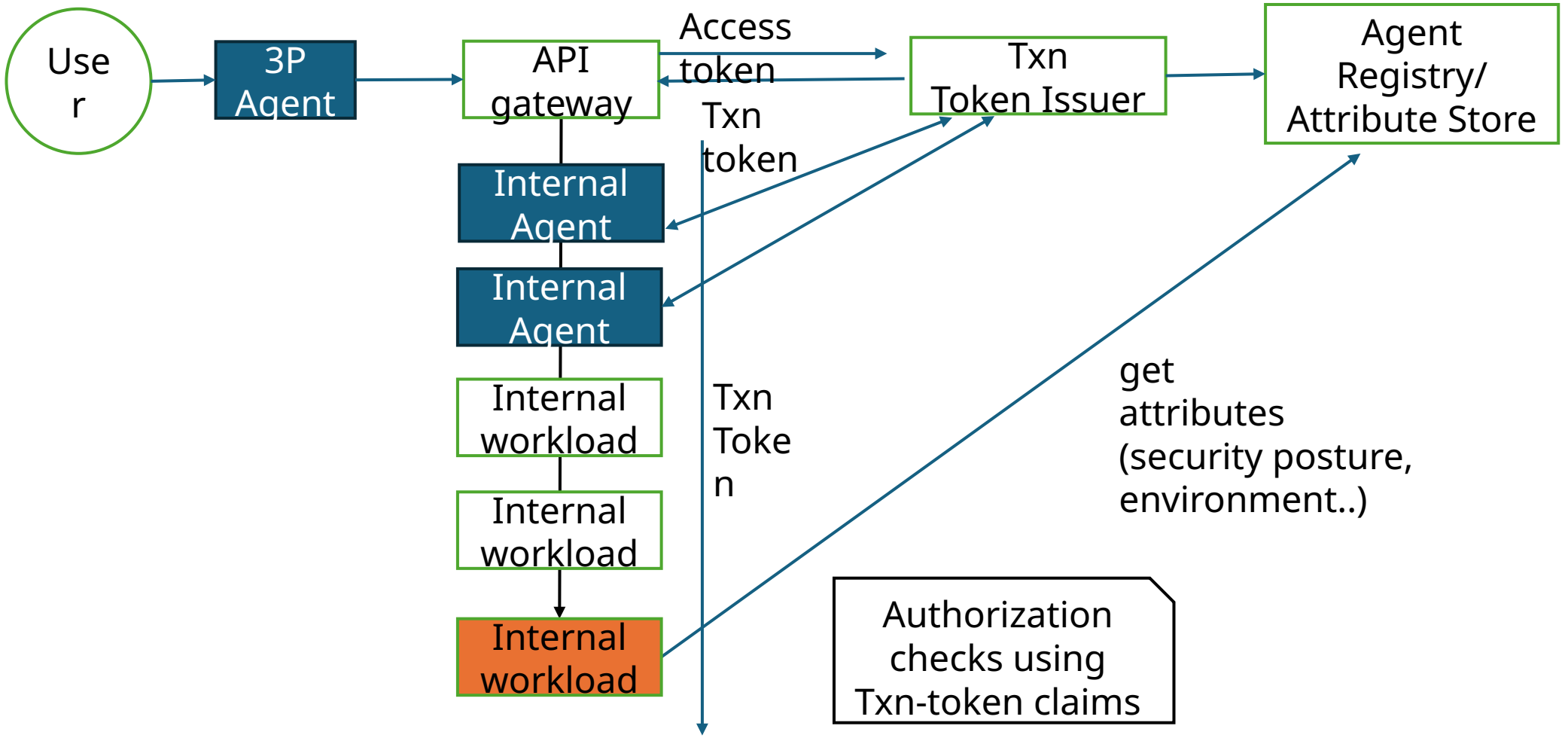
Proposal: New ‘agentic’ & ‘act’ claims in Txn-Token



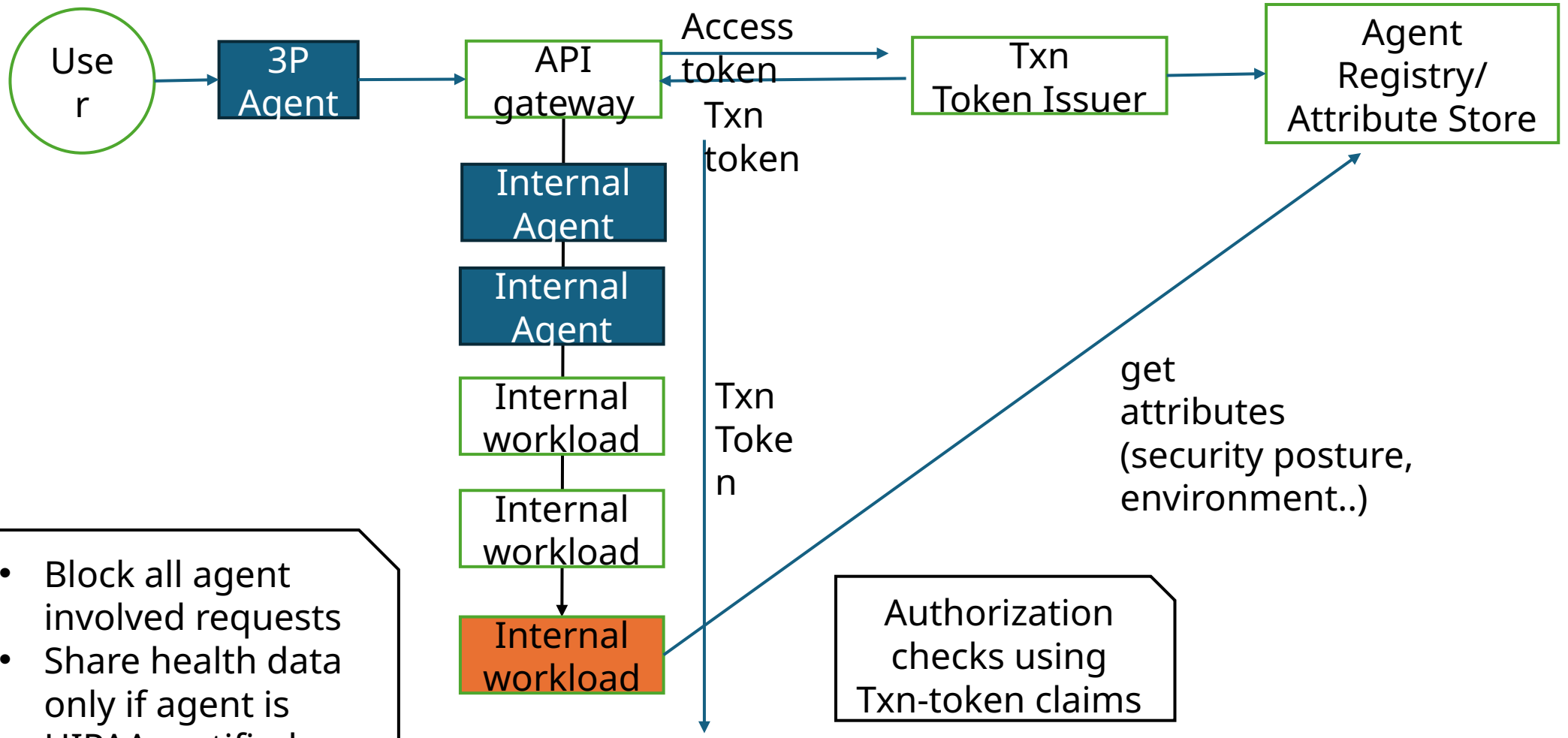
Proposal: New ‘agentic’ & ‘act’ claims in Txn-Token



Proposal: New ‘agentic’ & ‘act’ claims in Txn-Token



Proposal: New ‘agentic’ & ‘act’ claims in Txn-Token



agentic_ctx and *act* claims in Txn-Token

```
{
  “sub”: User
  “act”: 3P agent from access token
  “agentic_ctx": {
   "proximate_agent": {
      "id": "agent-identity-1",
       "session_id": "sess-3p-f4a2b8c1e990"
    },
    "originator": {
      "id": "agent-identity-1",
      "session_id": "sess-3p-f4a2b8c1e990"
     },
    "chain_metadata": {
      "hop_count": 1,
      "min_assurance_level": "low”
     },
   "attr_store_ref": https://registry.trust-domain.example/agents.
                          // isHIPAACertified, Prod/Pre-prod, Model versions,
posture, etc
    }
}
```

Security considerations

- **Identity laundering –** preventing by monotonic attenuation of *min_assurance_level* and immutable *originator.id/act*. A low trust origin cannot gain trust by routing from high trust agent.

- **Token exchange at agents** must happen at infrastructure layer (not LLM influenced paths)
  - Example – UserInputSubmit hook / middleware

- **Agentic call chain** is maintained in Txn token issuer logs. Helps with offline analysis.

- **Egress hygiene -** Strip *attr_store_ref* and internal identifiers before a token crosses a trust boundary.

- **Agent Attribute Store Integrity –** Access must be restricted and changes audited.

Best Current Practices for Transaction Tokens

draft-araut-oauth-transactiontokens-bcp-00

- **Token size and lifetime** – TTL to 5min and less. Never auto-renew expired token. Limit to 4KB and less. Monitor size at Txn Token Issuer Service. Relocate context to central attribute store.
- **Schema Governance** (Hyrum's law) – Unlike other Oauth tokens, Txn-token flows everywhere. Govern `tctx` and `agentic_ctx`. All workloads should register their policies in a centralized store. Modify schemas keeping backward compatibility in mind.
- **Token Propagation** – Set boundaries. Exchange token to remove/add contexts if required.
- **Asynchronous flows** – Draft propose uses of batch tokens to preserve contexts across workflows and event/subscriber flows.
- **Observability** – Central telemetry endpoint and metrics from SDKs to identify issuance, propagation, and token validation/decoding failures in your call chains.
  - Deeper and larger the call chains, bigger the challenge to ensure token coverage.
- **Key management** – Covers best practices for distributing keys across call chains.

What’s here and more to come?

- Industry implementations
- Collaborate with Cross domain transaction token work to propagate agentic context across trust domains
- Incorporate OAuth Actor profile extension
- New requests
  - delegation_ctx
  - Asserting session_id in a better trustworthy way
  - Provenance information (include all agent ids or not?)
  - Agent registry details

Thank you

Links

- BCP https://www.ietf.org/archive/id/draft-araut-oauth-transactiontokens-bcp-00.html
- Txn Token For Agents https://www.ietf.org/archive/id/draft-araut-oauth-transaction-tokens-for-agents-03.html
- Github https://github.com/ashayraut/oauth-transactiontokens-for-agents

Reach out to me here

