IETF 119
March 20, 2024

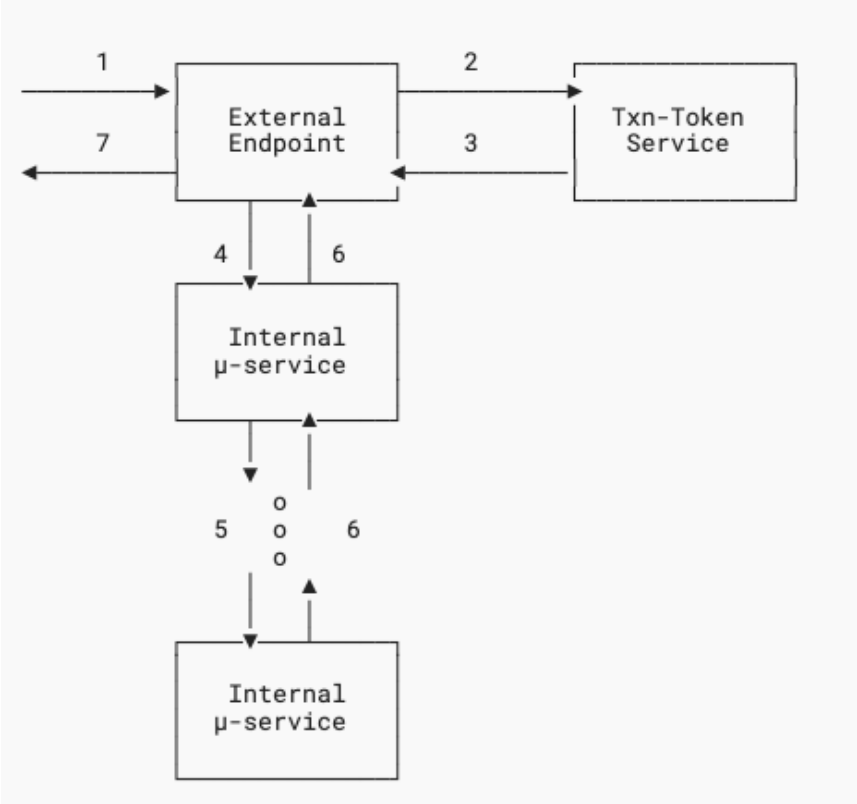
Atul Tulshibagwale
George Fletcher
Pieter Kasselman

Transaction Tokens

Updates in draft 01

Transaction Tokens

- Token internal to a given trust boundary
- Maintains the immutable context of a transaction
  - Subject
  - Context
  - Authorization Details
- Shared across multiple workloads
- Allows for “down-scoping” a transaction at the edge
- Supports finer-grained authorization



Restructured the Txn-Token Format section

- Re-organized the section
- Returned to a simple `sub` claim which MUST be unique within the context of the trust domain as defined by the `aud` claim
- `iss` claim is now optional
- Added section on how to manage a set or requesting workloads if one or more replacement Txn-Tokens are obtained

Requesting workload identifiers

Treat the `req_wl` claim a bit like an XFF header

If only one requesting workload, the value is a StringOrURI

If a replacement Txn-Token is requested, then convert the `req_wl` claim to an array and append the new requesting workload identifier

"req_wl": ["apigateway.trust-domain.example", "workload3.trust-domain.example"]

Txn-Token Request (section 7.1)

- Clarified that Txn-Tokens can be requested for both external driven transactions as well as internally driven ones
- Clarified that the subject_token and subject_token_type parameters are required but can contain simple values
- Clarified in section 7.1 the profile of RFC 8693 (Token Exchange)

Txn-Token Request Processing (section 7.2)

New section defining processing rules for the Transaction Token Service (TTS)

- Requesting workload authentication required
- Subject_token validation required
- The TTS must ensure the requesting workload is authorized to obtain the requested Txn-Token
- Provide flexibility for the TTS to make authorization decisions about what claim in the `request_context` and `request_details` should be put in the Txn-Token

Txn-Token Response (section 7.3)

- Clarified the profiling of RFC 8693 (Token Exchange)
- `token_type` must be set to N_A
- `issued_token_type` must be set to `urn:ietf:params:oauth:token-type:txn-token`

Creating replacement Txn-Tokens (section 7.4)

- Updated text to clarify that both the `sub` and `aud` claims MUST NOT be changed
- Added text to require the requesting workload identifier be added to the `req_wl` claim in the `rctx` object

Using Txn-Tokens (section 8)

- Added a section describing the presentation of the Txn-Token in an HTTP header for HTTP based requests

Question:

- Should we register a new HTTP header for passing the Txn-Token for HTTP requests?

Security Considerations

Added section 9.3 - Client Authentication

- Adds some guidance if the Token Exchange `actor_token` and `actor_token_type` parameters are used for client authentication.
- How a requesting workload authenticates to the Transaction Token Service is out of scope for this specification

Acknowledgements

Thank you to all those who have filed issues, commented on PRs or otherwise contributed to the work!