Transaction Tokens Update

G. Fletcher
P. Kasselman
A. Tulshibagwale

IETF 120

Updates since IETF 119

PR #73 - Cardinality of txn-token services

Added text to clarify that the trust domain will have only one logical transaction token service.

PR#86 Privacy considerations

Transaction tokens may contain PI or PII and as such, SHOULD NOT be logged in clear text. Other transformations can be performed to address logging.

PR#87 Replacement transaction tokens

Clarified the responsibilities of the Transaction Token Service when issuing replacement transaction tokens.

- MUST NOT modify ‘sub’ and ‘aud’ claims

PR#89 Clarify the `aud` claim in the transaction token

Clarified that the `aud` claim of the transaction token must be an identifier that uniquely identifies the trust domain.

Also clarified that the `sub` claim is unique within the context of the trust domain identifier.

PR#90 Self-signed JWTs as subect_tokens

Added text requiring workloads that require a transaction token and don’t have an appropriate token (e.g. OAuth access_token) to create a self-signed JWT containing the claims needed by the Transaction Token Service.

Definition of claims for this self-signed JWT is out of scope for this specification.

PR#92/103 clarified fields vs claims & IANA registry name

Defined the `txntoken+jwt` string to represent the `typ` value of the transaction token.

Register `urn:ietf:params:oauth:token-type:txn_token`

Register `Txn-Token` as the HTTP header for conveying Transaction Tokens

PR#99 Clarify the `azd` claim

Added a sub-section for the `azd` claim to clarify it’s intent and separate it from the `rctx` claim.

Cleaned up the examples

PR#100 Clarifies `scope` and processing logic

Clarified that scope can not be increased during replacement transaction token processing.

Clarified processing rules for workloads receiving a replacement transaction token (verify both signature and requesting workload identity)

PR#101 clarified use of the `txn` claim

Clarified that the `txn` claim is required and that if within a given deployment, a unique identifier can not be generated, then a fixed value of “N_A” MUST be supplied.

PR#102 clarified `purp` claim

Added a sub-section for the `purp` (purpose) claim and how it is different from most scope values.

PR#105 Added HTTP Header registration requirements

Spec text to define the Txn-Token HTTP header to be used to transport the transaction token within an HTTP request.

Current Topics Under Discussion

Should internal use cases require a self-signed JWT?

Or should this be kept out of scope and be deployment specific?

Issue#80 Extensibility of `azd` and `rctx`

Is an IANA registry required for extending these claims? The values here are often unique to the specific trust domain.

Should a deployment for a specific trust domain be able to define its own claims without registering them?

Issue#95 Discovery of Transaction Token deployment

Do we need to define discovery metadata for the Transaction Token Service and other aspects of the transaction token deployment?

Issue#96 Transaction Token deployment models

Should the specification discuss common (or best practice?) deployment models for transaction tokens?