Security Event Token (SET)

draft-ietf-secevent-token

Michael B. Jones
IETF 99, Prague
July 2017
Status Review

- Current version draft-ietf-secevent-token-02
- Functionality stable
- Edits since IETF 98 have addressed the issues discussed there and on the list
Updates Since IETF 98

- Described how to prevent confusion of SETs with ID Tokens, access tokens, and other kinds of JWTs
- Registered “application/secevent+jwt” content type and defined how to use it for explicit typing of SETs
- Noted that some SET profiles may choose to place event subject info in the event payload
- Added Requirements for SET Profiles section
Preventing Confusion of SETs with ID Tokens

- The “exp” claim is to be omitted from SETs
  - Because “exp” is required in ID Tokens, existing ID Token validation code will reject SETs
- *This is actually defense in depth*
  - Not having a valid “nonce” value already prevents confusion
Explicit Typing Added

- The "application/secevent+jwt" content type is defined to enable explicit typing of SETs using the "typ" header parameter
- Aligns with guidance in proposed JWT BCP
  - draft-sheffer-oauth-jwt-bcp
Status and Next Steps

- Functionality has been stable for most of a year
- Meets the needs of known use cases
- Vigorous discussions since IETF 98 generated solutions to the previously open issues

- Several have already stated on the list that it’s time for Working Group Last Call
  - I agree with this assessment