Security Event Token (SET) Issues Discussion

draft-ietf-secevent-token

Michael B. Jones

IETF 98, Chicago
March 2017

Status Review

- Current version draft-ietf-secevent-token-01
- Semantics stable
- Recent edits have clarified exposition
- Many recent review comments already addressed
- Some issues still being discussed
  - These issues the subjects of the next 9 slides

Terminology Change

- Terminology recently changed to “Event Transmitter” and “Event Receiver”
  - Changed from “Publisher” and “Subscriber”
  - Happened between -00 and -01

- Which terminology do people prefer?

Claims vs. Commands

- Discussion on whether it’s meaningful to say that SETs can’t represent commands
  - See e-mail thread “Statement of historical fact, command, or distinction without a difference?”
- New proposed wording talks about intentions rather than unenforceable restrictions
  - Wording like that seems to have support

Using “claims” terminology rather than “facts”

- Proposal made to talk about “claims” rather than “facts”
  - Also see thread “Statement of historical fact, command, or distinction without a difference?”
- “Claims” is standard JWT terminology already in widespread use by the SET spec
- Support for change to “claims” voiced on list

Possible confusion of SETs with ID Tokens

- Both are JWTs, with different profiles
  - See the thread “Thread: Clarifying use of sub and iss in SET tokens”
- They have different claims
  - “nonce” vs. “events”, etc.
- As recently discussed by Connect WG, even if a SET had a nonce, it’s value wouldn’t match, so prohibiting “nonce” unnecessary
- ID Token/SET confusion not actual problem

Possible confusion of SETs with access tokens

- RFC 6749 defines access token format as unspecified
  - Therefore, unsolvable in general case
- Some access tokens are JWTs
  - Several techniques can be used to distinguish
    - Use different “aud” (audience) values
    - Use presence of “events” claim to distinguish
    - Use lack of access token claims to distinguish
  - We could describe these techniques in the Security Considerations section

Use of the “aud” claim

- Some people have proposed restrictions for audience syntax
  - For instance, requiring that values be URIs
- Others have stated that it’s up to profiles to define what values make sense
  - For instance, sometimes “aud” is a Client ID
- Restrictions would limit applicability of SETs

Use of the “sub” claim

- Some people have proposed restrictions for subject syntax and requiring its use
  - For instance, requiring that values be URIs
- Others have stated that it’s up to profiles to define what values make sense
  - For instance, sometimes “sub” is issuer-relative
- Sometimes “sub” isn’t needed at all
  - For instance, when the subject is the issuer

- Restrictions would limit applicability of SETs

Use of the “exp” claim

- Spec currently recommends against its use
- Some have asked to be able to use it to bound SET token caching lifetime
  - This is an intended use of “exp”
- It would be reasonable to leave this decision up to SET profiles, like other claims

Use of the “iss” claim

- Sometimes “iss”/“sub” pair identifies event subject and event issuer “iss” value different
    - In that case, an “iss” and “sub” would be in the event payload
- Some asked, why not always put them there?
    - Others objected to required data duplication
- Sometimes all you need is a single “iss” value
    - When the event issuer is authoritative for the event subject
    - Some use cases already use SET that way

Next Steps

- Discuss and decide issues
- Then time for Working Group Last Call?
  - Charter milestones include WGLC by June 2017