Push-Based SET Token Delivery Using HTTP

Annabelle Backman

IETF 103 – November 2018
POST /Events HTTP/1.1
Host: recipient.example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
Content-Type: application/secevent+jwt

...SET in request body...
Success Response

HTTP/1.1 202 Accepted
HTTP/1.1 400 Bad Request
Content-Type: application/json

{
  "err": "jwtAud",
  "description": "Invalid audience value."
}
Current Status

• 03 draft published 2018-10-18

• Implementations:
  • Google
    • Transmitter: Implemented
    • Receiver: In progress?
  • Amazon
    • Receiver: In progress
    • Transmitter: In progress
• Rewrote abstract, introduction, protocol technical description.

• Removed redundant, unnecessary text.

• Minor normative corrections.

• Added IANA registry for error codes.
Push/Poll Duplication Reduction

- Definitions
  - Both reference 8417 and define Event Transmitter.

- Failure response structure
  - `{ "err": "...", "description": "..." }`

- Security Considerations

- Privacy Considerations
Open Item: Error Codes

• Current list of errors are poorly differentiated.
  • If decryption produces garbage, is it a json, jwtParse, or jwe error?
  • Is an incomplete event payload setParse or setData?

• Mostly JWT errors, not SET errors
  • Syntax
  • JWE and JWS processing
  • JWT constraint validation
## Error Codes: JWT vs. SET

<table>
<thead>
<tr>
<th>json</th>
<th>jwtAud</th>
</tr>
</thead>
<tbody>
<tr>
<td>jwtParse</td>
<td>jwtIss</td>
</tr>
<tr>
<td>jwtHdr</td>
<td>setType</td>
</tr>
<tr>
<td>jwtCrypto</td>
<td>setParse</td>
</tr>
<tr>
<td>jws</td>
<td>setData</td>
</tr>
<tr>
<td>jwe</td>
<td>dup</td>
</tr>
</tbody>
</table>
Revised Error Codes: JWT vs. SET

<table>
<thead>
<tr>
<th>jwt-malformed</th>
<th>jws-key-invalid</th>
</tr>
</thead>
<tbody>
<tr>
<td>jwt-header-invalid</td>
<td>jws-alg-invalid</td>
</tr>
<tr>
<td>jwt-expired</td>
<td>jws-error</td>
</tr>
<tr>
<td>iss-invalid</td>
<td>jws-mismatch</td>
</tr>
<tr>
<td>aud-invalid</td>
<td>event-missing</td>
</tr>
<tr>
<td>jwe-key-invalid</td>
<td>event-invalid</td>
</tr>
<tr>
<td>jwe-alg-invalid</td>
<td>payload-invalid</td>
</tr>
<tr>
<td>jwe-error</td>
<td>...</td>
</tr>
</tbody>
</table>
JWT Errors vs. SET Errors

- Existing JWT error code definitions?
- Is this draft the right place to define them?
- Is secevent the right WG?
- Reopen the JOSE WG?