SET Token Delivery Using HTTP

Annabelle Backman

IETF 101 – March 2018

SET Token Delivery Using HTTP

- draft-ietf-secevent-delivery-02

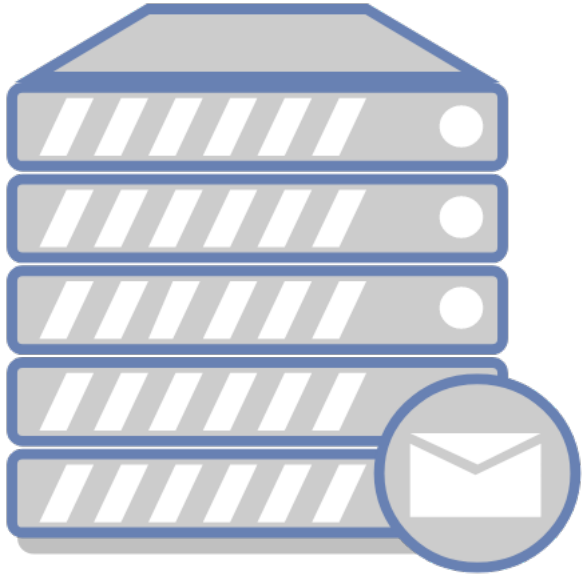
- Terminology:
  - Event Transmitter: Party that has the SET.
  - Event Receiver: Party that wants the SET.

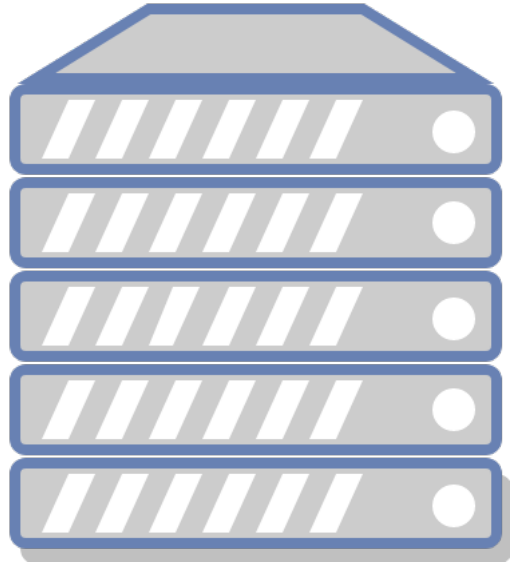
- Two mechanisms for transmitting SETs over HTTP:
  - Push: Transmitter sends to Receiver
  - Poll: Receiver pulls from Transmitter

HTTP Push

- Transmitter sends SET to Receiver
- Receiver replies with 202 or 400.

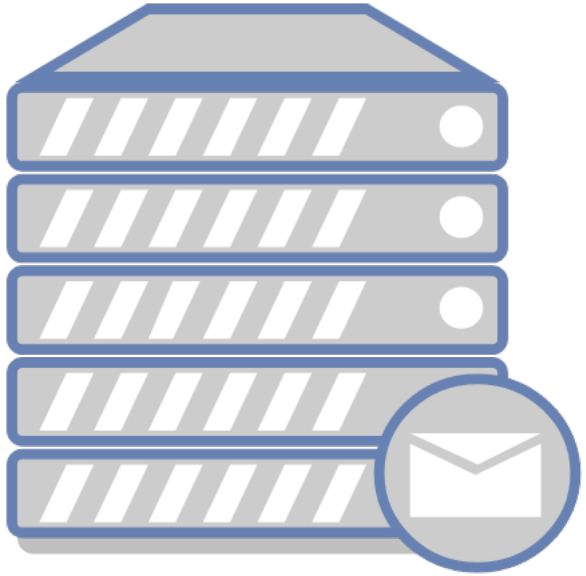
HTTP Push

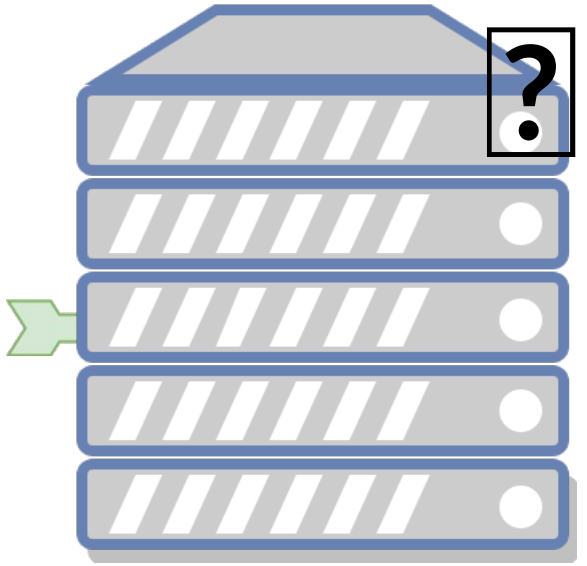




```
POST /Events HTTP/1.1
Host: receiver.example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
Content-Type: application/secevent+jwt


...SET in request body...
```

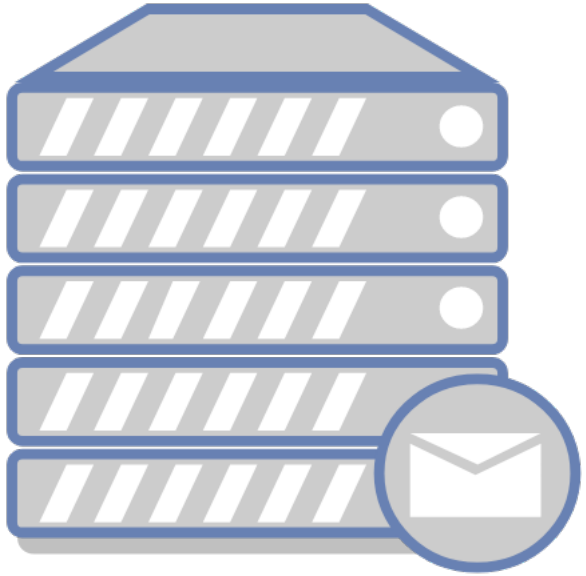
HTTP Push

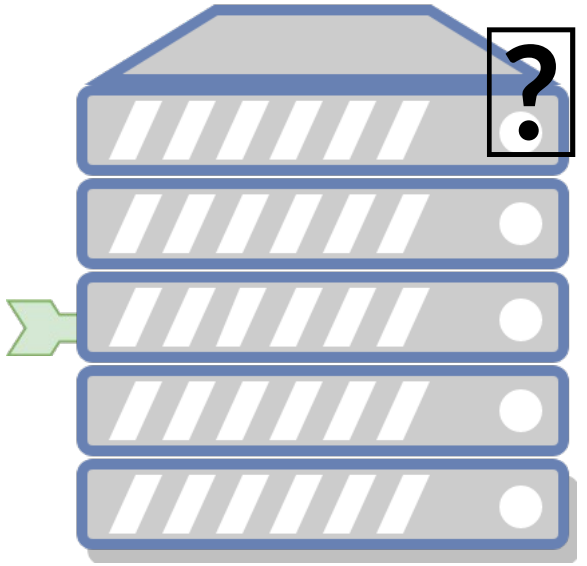





```
HTTP/1.1 202 Accepted
```

HTTP Push



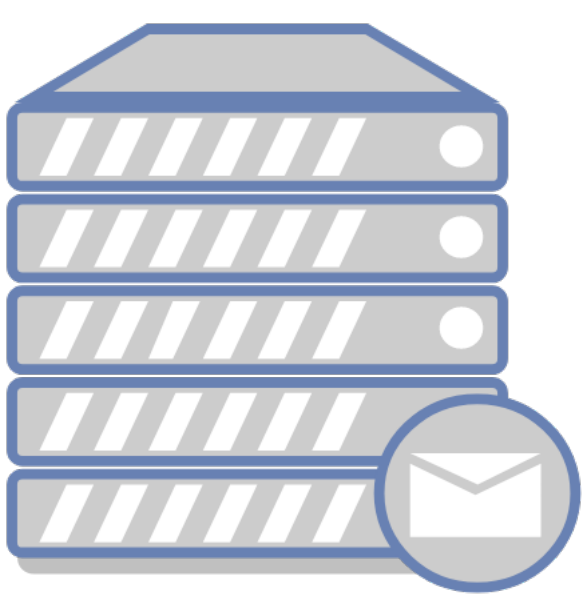


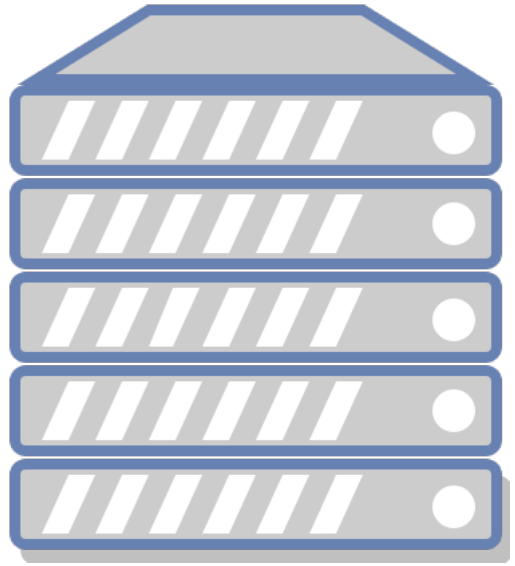

```
HTTP/1.1 400 Bad Request
Content-Type: application/json


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

HTTP Poll

- Receiver asks Transmitter for SETs.
- Receiver acknowledges SETs in a later request.

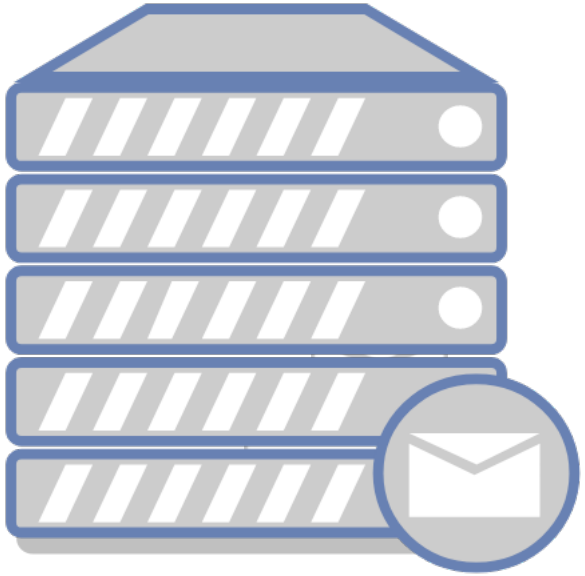
HTTP Poll

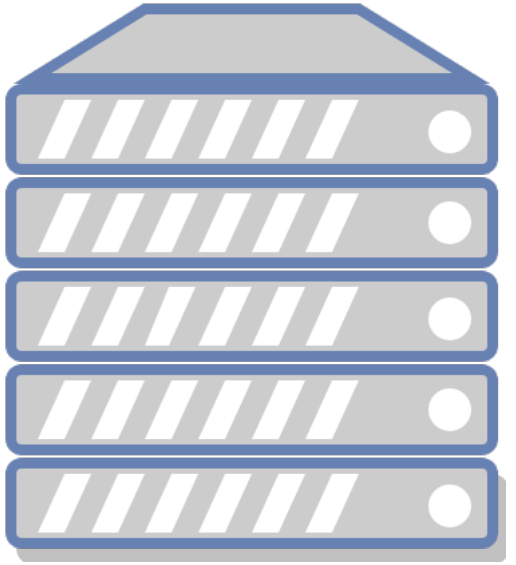




```
POST /Events HTTP/1.1
Host: transmitter.example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
Content-Type: application/json

{
  "returnImmediately":false
}
```

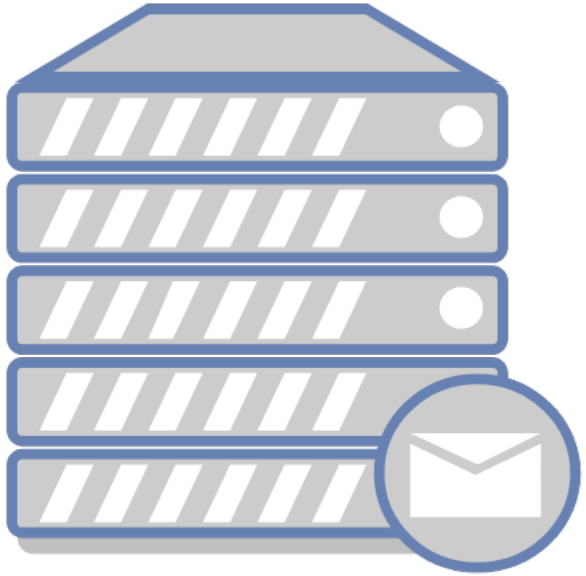
HTTP Poll

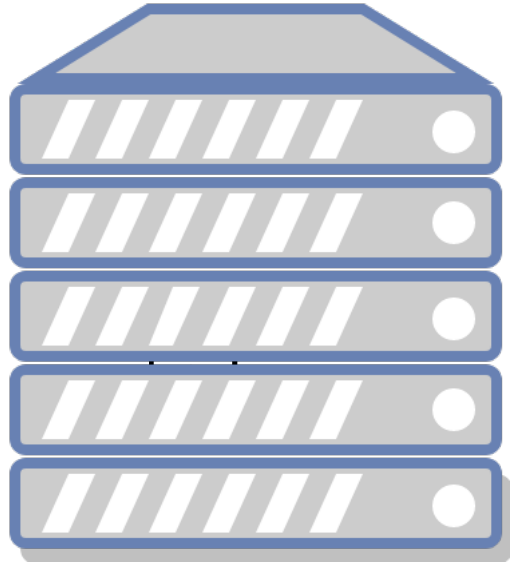




```
HTTP/1.1 200 OK
Content-Type: application/json


{
  "sets": {
    set_jti_1: set_1,
    ...
  }
}
```

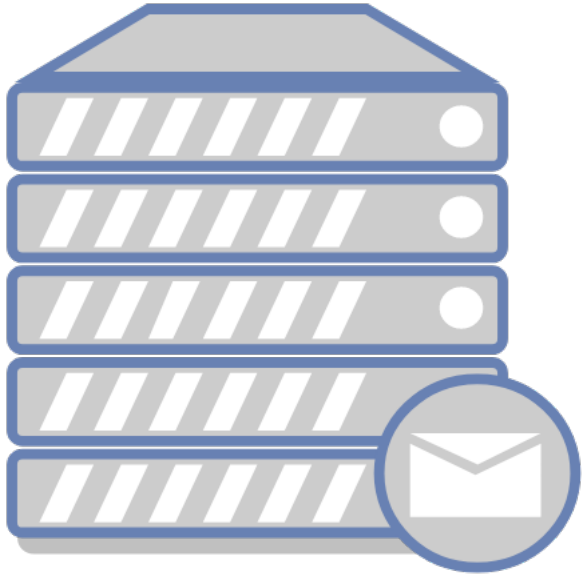
HTTP Poll

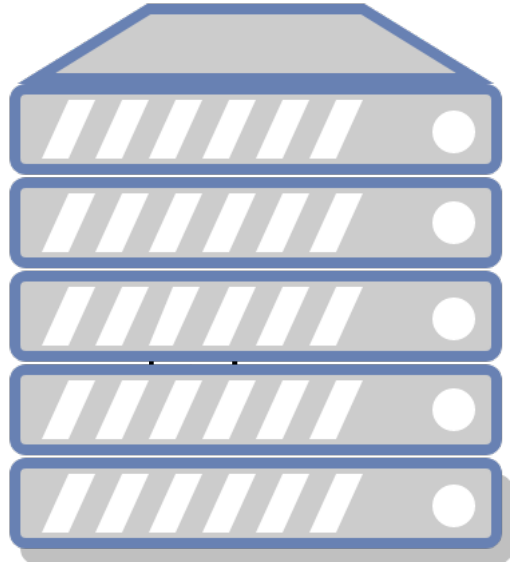




```
POST /Events HTTP/1.1
Host: transmitter.example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
Content-Type: application/json


{
  "ack": [ set_jti_1, set_jti_2, ..., set_jti_n ]
}
```

HTTP Poll





```
POST /Events HTTP/1.1
Host: transmitter.example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
Content-Type: application/json


{
  "setErr": { set_jti_1: set_err_1, ... }
}
```

HTTP Poll

```
POST /Events HTTP/1.1
Host: transmitter.example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
Content-Type: application/json


{
  "maxEvents": 10,
  "returnImmediately": false,
  "ack": [ set_jti_1, set_jti_2, ..., set_jti_n ],
  "setErr": { set_jti_1: set_err_1, ... }
}
```

Current Status

- 02 draft published 2018-03-04

- Open issues:
  - HTTP status codes for error responses
  - Which method is MTI?

- Implementations:
  - Google: HTTP Push implemented
  - Amazon: HTTP Push in progress
  - Microsoft: HTTP Poll in progress/implemented (?)

HTTP status codes for error responses

Error response structure:

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

HTTP status codes for error responses

err	Description	HTTP Status Code
`json`	Invalid JSON object.	400
`jwtParse`	Invalid or unparsable JWT or JSON structure.	
`jwtHdr`	In invalid JWT header was detected.	
`jwtCrypto`	Unable to parse due to unsupported algorithm.	
`jws`	Signature was not validated.	
`jwe`	Unable to decrypt JWE encoded data.	
`jwtAud`	Invalid audience value.	
`jwtIss`	Issuer not recognized.	
`setType`	An unexpected Event type was received.	
`setParse`	Invalid structure was encountered.	
`setData`	SET event claims incomplete or invalid.	
`dup`	A duplicate SET was received and has been ignored.	

HTTP status codes for error responses

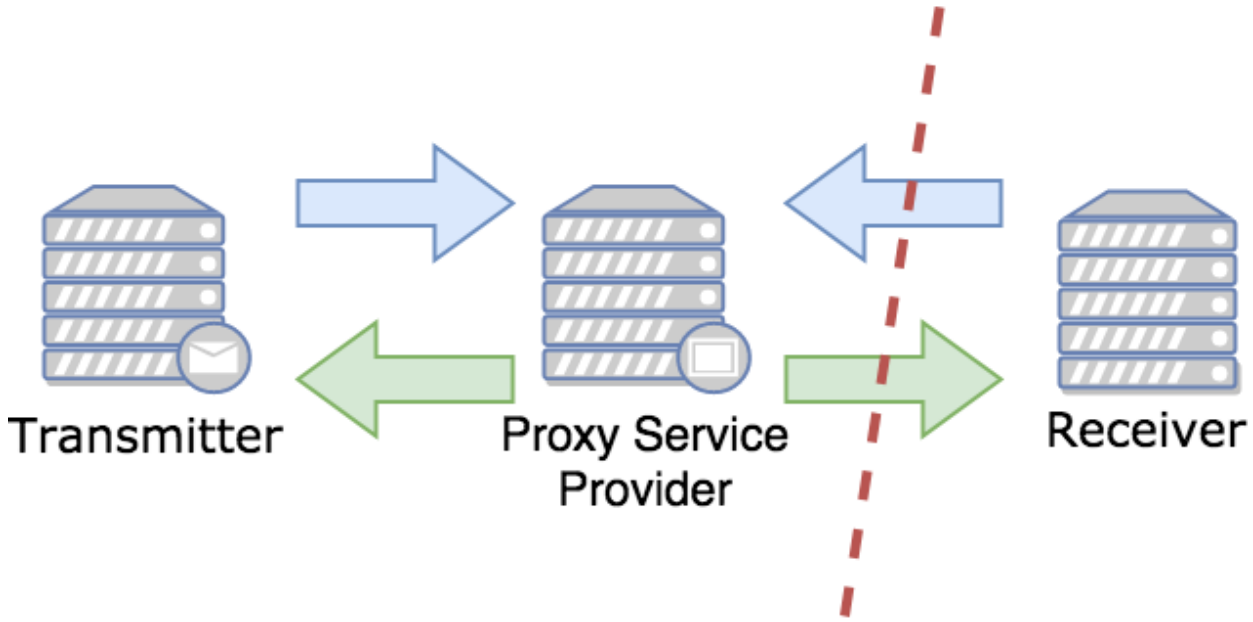
err	Description	HTTP Status Code
`json`	Invalid JSON object.	400
`jwtParse`	Invalid or unparsable JWT or JSON structure.	
`jwtHdr`	An invalid JWT header was detected.	
`jwtCrypto`	Unable to parse due to unsupported algorithm.	
`jws`	Signature was not validated.	
`jwe`	Unable to decrypt JWE encoded data.	
`jwtAud`	**Invalid audience value.**	**403**
`jwtIss`	**Issuer not recognized.**	
`setType`	An unexpected Event type was received.	400
`setParse`	Invalid structure was encountered.	
`setData`	SET event claims incomplete or invalid.	
~~**`dup`**~~	~~**A duplicate SET was received and has been ignored.**~~	~~**400**~~

Push vs. Poll: What is MTI?

	Push	Poll
Pros	• Very simple protocol.	• Works for "everyone."
Cons	• Receiver has to expose an endpoint.	• Transmitter has to persist all SETs. • More orchestration for receiver.

HTTP Poll by Proxy

- Push between Transmitter and Proxy.
- Poll between Proxy and Receiver.



Split the draft?

SECEVENTS: FURY ROAD

Fundamental Questions

- Can we define a single MTI protocol for "SET Delivery?"
- *Must* we define a single MTI protocol for "SET Delivery?"
- Who is this protocol for?