野村総合研究所

NRI 未来創発
Dream up the future.

IETF 101 #OAuth WG

OAuth Response Metadata

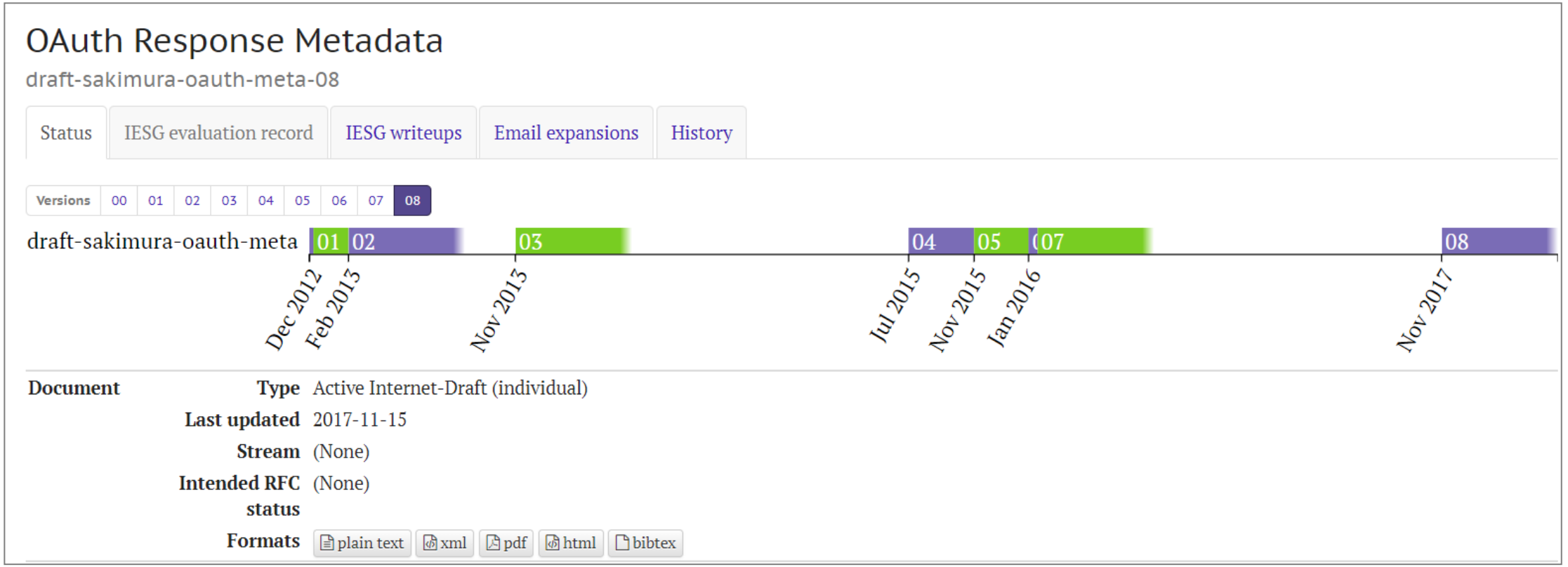
draft-sakimura-oauth-meta

2018-03-21

Nat Sakimura, Nomura Research Institute

OAuth Response Metadata is a generic framework that has been floating around for 6 years.
It can be used to indicate to the client such metadata as:

- Resource Server Metadata, e.g., who is the acceptable AS, and what scope is needed.
- Authorization Serer Response metadata, e.g., on which RS, the token can be used.



The scope of draft-Sakimura-oauth-meta and draft-hardt-distributed-oauth is not dissimilar.

draft-hardt-distributed-oauth

- Target
  - Client Credential Flow
- Enables a client to find out
  - the location of the token endpoint;
  - the scope the AS supports;

draft-sakimura-oauth-meta

- Target
  - Any Flow in OAuth
- Enables a client to find out
  - the server metadata;
  - the location of the Authorization endpoints, token endpoints, discovery endpoints, etc.

Approaches are not dis-similar

Both leverages the `401 Unauthorizaed` error response with `WWW-Authenticate` [RFC7235] header to bootstrap the flow.

draft-hardt-distributed-oauth-00

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer realm="example_realm",
iss="http://issuer.example.com/token", scope="example_scope",
error="invalid_token"
```

Extends `WWW-Authenticate` header.
Only for Token Endpoint.

draft-sakimura-oauth-meta-08

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer realm="example_realm"
Link: <https://example.com/.well-known/oauth-authorization-server>; rel="duri",
        <https://example.com/authz/>; rel="auri"; scope="example_scope",
        <https://example.com/token/>; rel="turi"
```

Leverages RFC5988 Web Linking and OAuth Response Metadata.
Advantage: The same mechanism can be used by other endpoints.
Discussion: Perhaps better to use JSON version instead. (It was in the earlier draft and they are gaining popularity these days.)

-08 does not but it should define 'scope' as a 'Target Attribute'.

Relationships to other documents

- draft-campbell-oauth-resource-indicators
  - Indicates to Token Endpoint to which RS the client is going to use the token so that the token endpoint can mint an appropriately scoped and formatted access token.

```
POST /as/token.oauth2 HTTP/1.1
    Host: authorization-server.example.com
    Authorization: Basic czZCaGRSa3F0Mzpoc3FFelFsVW9IQUU5cHg0RlNyNHlJ
    Content-Type: application/x-www-form-urlencoded

    grant_type=refresh_token
    &refresh_token=4LTC8lb0acc6Oy4esc1Nk9BWC0imAwH
    &resource=https%3A%2F%2Frs.example.com%2F
```

Perhaps complementary to draft-sakimura-oauth-meta.
It is dealing with the "request" (both authorization and token) while OAuth Response Metadata is about the response.

- draft-tschofenig-oauth-audience
  - Defines a new header that is used by the client to indicate what resource server, as the intended recipient, it wants to access. This information is subsequently also communicated by the authorization server securely to the resource server, for example within the audience field of the access token.

Already merged with the above?

Maybe merge them together in a single new work item?