GNAP Interim Meeting

draft-ietf-gnap-core-protocol-03

January 12, 2021

Justin Richer • Aaron Parecki • Fabien Imbault

Agenda

- Updates on Latest Draft (-03)
  - Terminology
  - Functional changes
  - Editorial changes
- Issues
  - #40 access token request/response format
  - #122 interaction request/response format

Terminology

- Goal: enable future technical work with more clarity
- Takes into account discussions/feedbacks on the mailing list
- ISO style (definition, note, example)
- Provide self-contained definitions (no embedded requirement, no circular def)
- Don’t change what works / what people know (AS, RS, client), but be precise
- Issue #29 / PR #155 (pending merge) / wiki

Future steps:

- Identify if we need additional terms (ex: interaction server, key proof, etc.) - would be managed through dedicated issues

Terminology : list of terms

- roles:
  - AS / client / RS / RO / end-user
- elements:
  - attribute / access token / grant / privilege / protected resource / right / subject / subject information

- changed: RQ -> end-user
- included (sub-definitions):
  - privilege / attribute / right / subject (cf https://tools.ietf.org/html/draft-ietf-secevent-subject-identifiers-06)
- removed:
  - cryptographic key (nothing specific to the spec)

Functional Changes

- Dropped redirect to a short URL (#139, #121, #53)
- Dropped OpenID Connect “claims” parameter (#140)
- Made access tokens mandatory for continuation request (#129, #67)

Editorial Changes

- Removed closed issues from draft text (#150)
- Fixed a bug about sub_ids (#153)
- Rephrased to “GNAP” instead of “GNAP protocol” (#125)
- Minor typo fixes (#126)
- Updated acknowledgements

Discussion Items

#40 Access Token Request/Response Format

https://github.com/ietf-wg-gnap/gnap-core-protocol/issues/40

Current Syntax: Request

```
{
  "client": ...
  "resources": [
    {
        "type": "photo-api",
        "actions": [ "read", "write", "dolphin" ],
        "locations": [
            "https://server.example.net/",
            "https://resource.local/other"
        ],
        "datatypes": [ "metadata", "images" ]
    },
    "read",
    "bind_token",
    "multi_token"
  ]
}
```

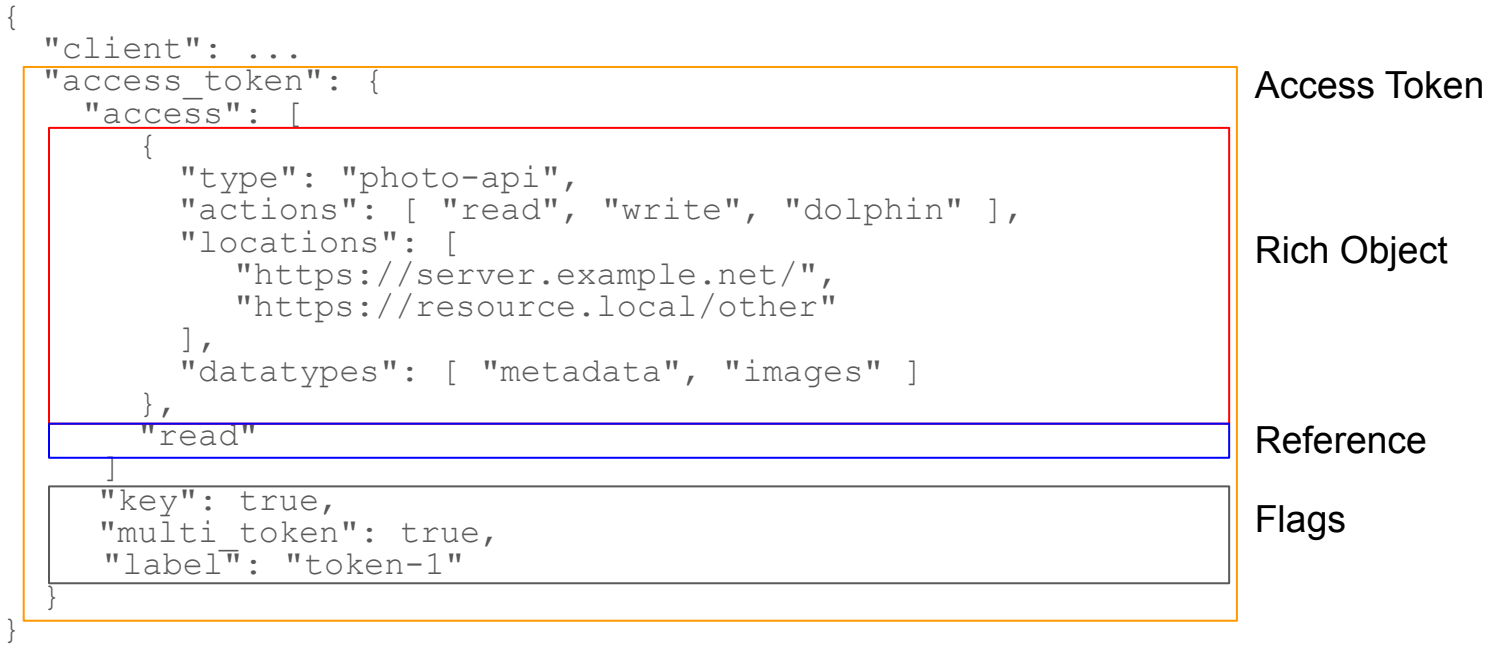
Access Token

Rich Object

Reference

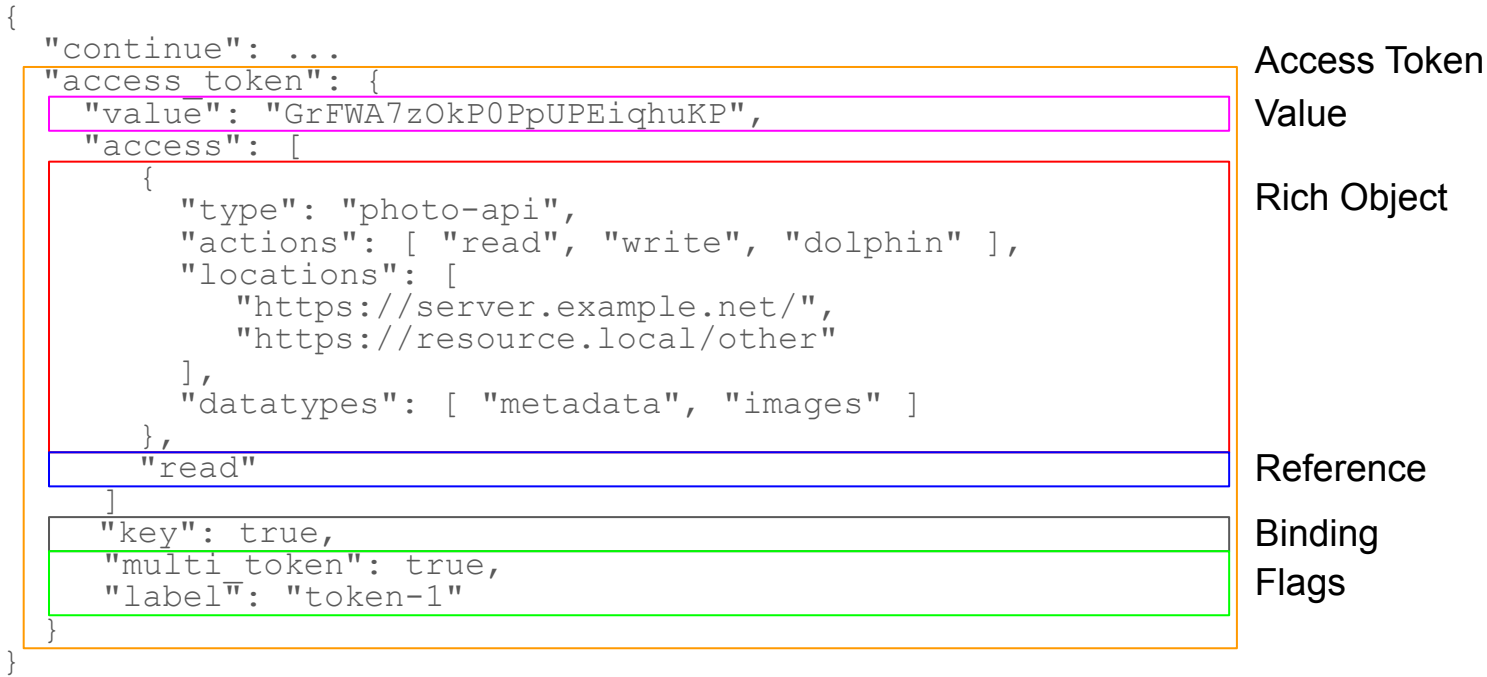
Flags

Proposed Syntax: Request



Current Syntax: Response

Proposed Syntax: Response



Current Syntax: Multi Request

```
{
  "client": ...
  "resources": {
    "token1": [ "write", "bind_token" ],
    "token2": [ "read" ]
  }
}
```

First, bound

Second, bearer

Proposed Syntax: Multi Request

```
{
  "client": ...
  "access_token": [
    {
      "label": "token1",
      "access": [ "write" ],
      "key": true
    },
    {
      "label": "token2",
      "access": [ "read" ],
      "key": false
     }
  ]
}
```

First, bound

Second, bearer

Current Syntax: Multi Response

```
{
  "continue": ...
  "multiple_access_tokens": {
    "token1": {
      "value": "GrFWA7zOkP0PpUPEiqhuKP",
      "resources": [ "write" ],
      "key": true
    },
    "token2": {
      "value": "PNEKgODQk/7vRW59sAden1",
      "resources": [ "read" ],
      "key": false
    }
  }
}
```

First, bound

Label in structure

Second, bearer

Proposed Syntax: Multi Response

First, bound

Label internal

Second, bearer

Why change?

- Parallelism between request and response
- Easier to talk about attributes other than “resources”
  - Including better defaults (ie, default to “bound” token)
- Paves the way for directed tokens
  - “Label” is just a start
- Consistent syntax for single/multi token requests

Downsides?

- More complex structure
- Requires separate “label” to differentiate multiple tokens

Interaction Request/Response Format

https://github.com/ietf-wg-gnap/gnap-core-protocol/issues/122

Current Syntax

```
"interact": {
  "redirect": true,
  "app": true,
  "user_code": true,
  "callback": {
    "method": "redirect",
    "uri": "https://client.example.net/return/123455",
    "nonce": "LKLTI25DK82FX4T4QFZC"
  },
  "ui_locales": ["en-US", "fr-CA"]
}
```

How the client can interact with the user

How the client can receive a response from the AS

Hints to the AS

Proposed Syntax

```
"interact": {
  "start": ["redirect", "app", "user_code"],
  "finish": {
    "callback":{
      "method": "redirect",
      "uri": "https://client.example.net/return/123455",
      "nonce": "LKLTI25DK82FX4T4QFZC"
    }
  },
  "hints": {
    "ui_locales": ["en-US","fr-CA"]
  }
}
```

Why change?

- Clearer to understand what the values mean when separating the start/finish parts of the flow
- Avoids boolean values when the only meaningful value is “true” anyway
- Future development and extensions don’t risk conflicts

```
"interact": {
  "start": ["redirect", "app", "user_code"],
  "finish": {
    "callback":{
      "method": "redirect",
      "uri": "https://client.example.net/return/123455",
      "nonce": "LKLTI25DK82FX4T4QFZC"
    }
  },
  "hints": {
    "ui_locales": ["en-US","fr-CA"]
  }
}
```