Resource Indicators for OAuth 2.0

Brian Campbell
John Bradley
Hannes Tschofenig

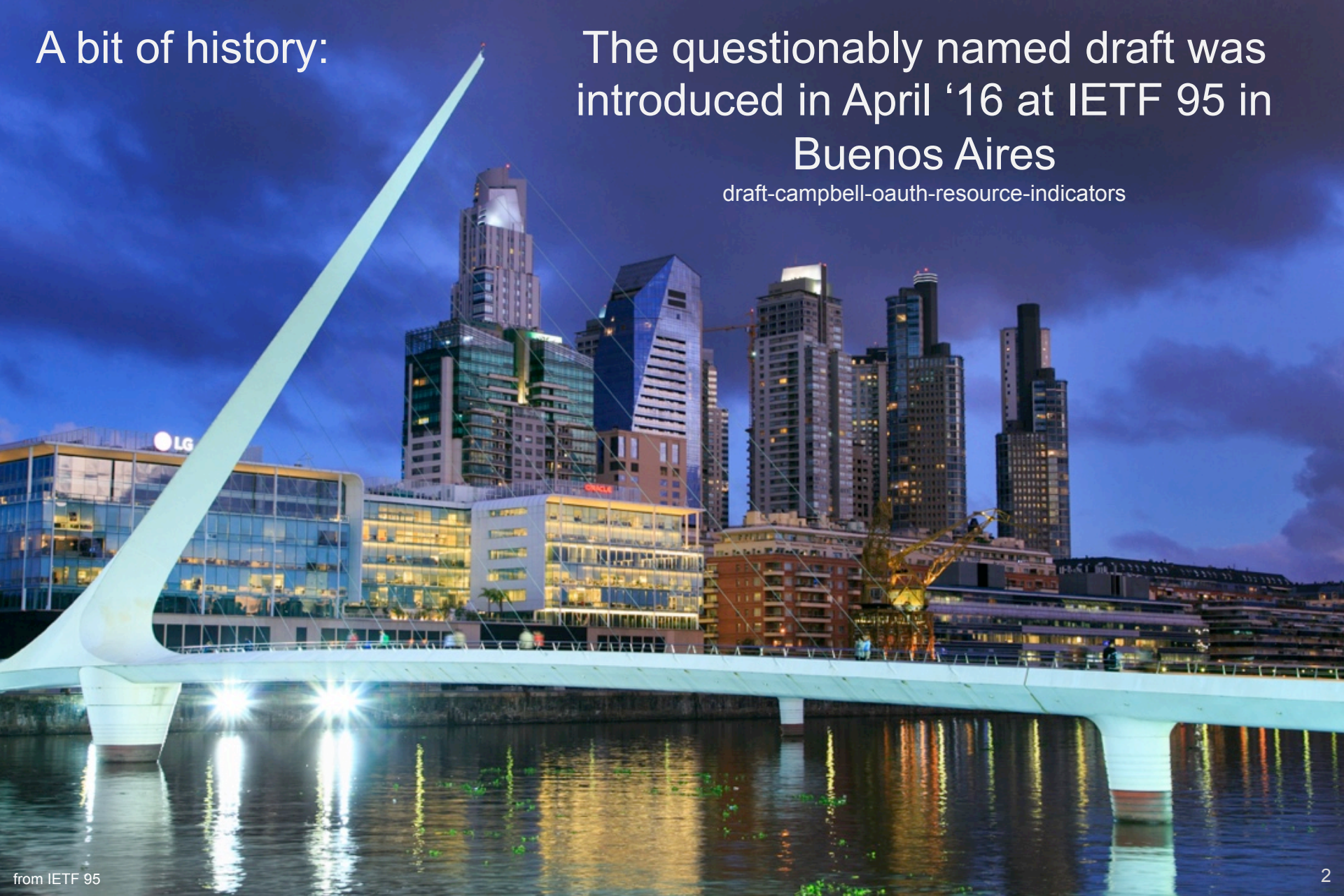
IETF 101
London
March 2018

https://tools.ietf.org/html/draft-campbell-oauth-resource-indicators-02

A bit of history:

The questionably named draft was introduced in April ‘16 at IETF 95 in Buenos Aires

draft-campbell-oauth-resource-indicators

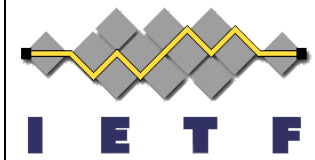


from IETF 95

What is [was] it?

- A new "`resource`" parameter(s)
  - URI where the client intends to use the access token
  - Applicable on the:
    - Authorization request for access tokens that will be returned from the authorization endpoint
    - Token request for for access tokens that will be returned from the token endpoint
    - Usage implies the resource is not persisted with the grant

Why?



- Enables access token to be minted appropriate to the target resource
  - Encryption, content/claims, reference vs. JWT, keys/algs, etc.
- Facilitates audience restricting access tokens
  - AS may use the exact "resource" value for audience or it may map to a more general URI or abstract identifier for the RS
- General concept has been discussed for some time
  - ‘audience’ in tschofenig-oauth-audience, ‘aud’ in oauth-pop-key-distribution, ‘resource’ & ‘audience’ in oauth-token-exchange
- Proprietary variations already exist and deployed
- Arguably a omission (conceptually anyway) of the original OAuth 2.0 ~~spec~~ Authorization Framework

Relation to Scope?

- Scope is ‘what’
  - Sometimes overloaded to convey the location of the resource server (or it is implied)
    - But not always feasible or desirable
- Resource is ‘where’
  - & allows for distinct treatment of ‘where’ from ‘what’

from IETF 95

Whatever became of it...

"Let it linger for a few years until the idea is resurrected in some other form?"

Next Steps?

- Please read (it's relatively short)
  - https://tools.ietf.org/html/draft-campbell-oauth-resource-indicators-01
- Feedback, changes, additions, vague & incomprehensible criticisms…
- Better title?
- Consideration as a WG document?
- Kill it?
- Let it linger for a few years until the idea is resurrected in some other form?
- Other?

5

[Docs] [txt|pdf|xml|html] [Tracker] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-hardt-distributed-oauth) 00

Network Working Group — D. Hardt
Internet-Draft — Amazon
Intended status: Standards Track — November 14, 2017
Expires: May 18, 2018

Distributed OAuth
draft-hardt-oauth-distributed-00

Abstract

The OAuth client credentials grant The Distributed OAuth profile enables an OAuth client using the client credentials grant to discover what authorization server to use for a given resource server, and what attribute values to provide in the access token request.

- Client discovers authorization server(s) from protected resource in HTTP 401 response
  - `iss` attribute in `WWW-Authenticate: Bearer` response header (note despite the name it's the token endpoint URL not the issuer)
- `host` parameter passed in access token request
  - `client_credentials` grant only
  - `host` claim/attribute placed in issued access token and verified in protected resource access

So now what?

- I dunno...
- But let's please not unduly constrain potentially useful and generally applicable functionality/concepts