*

can prevent malicious forwarding
or redirection of JWTs with a

Destination Claim for JWT

Destination Claim for JSON Web Token
draft-campbell-oauth-dst4jwt

Brian Campbell
IETF #92
Dallas
March 2015

* "Smokey3" by Forest Service, United States Department of Agriculture, in cooperation with the Association of State Foresters and the Advertising Council - http://gis.nwcg.gov/gist_2004/logos/federal_logos.html. Licensed under Public Domain via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Smokey3.jpg#/media/File:Smokey3.jpg

What is it?

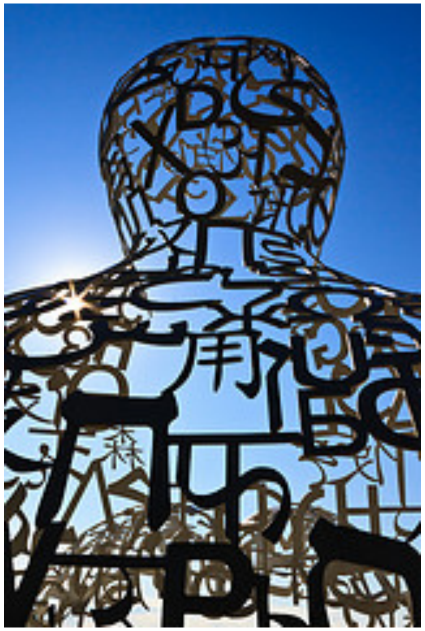
- A new JWT claim
  - “dst” short for “destination”
- Indicates the address to which a JWT is sent
- Issuer can say where they’re sending the JWT
- Recipient can check that the location the JWT was sent is the same as the location at which it was actually received

Why Bother?

- JWTs are being used a lot
  - a lot
- In a variety of ways
  - beyond OAuth 2.0 Access Tokens and OpenID Connect ID Tokens
- Sometimes transferred via an HTTP 302 redirect or an auto-submitted HTML form using the browser as a intermediary
  - Potentially vulnerable malicious forwarding or redirection by the user or via XSRF
- “dst” can help

But isn’t that the same as Audience?

- Similar?
  - yes.
- Same?
  - no.
- Audience -> *who*
  - + multivalued ‘or’ semantics
- Destination -> *where*
  - just one



Running Code

JWT claims scraped from a live deployment

```
{
 "iss": "pingone",
 "sub": "bcampbell",
 "aud": "pingidauthenticator",
 "nonce": "IDa64e5b0bba2b3dd363dadd1a2e695c103d615637c73d4ee103",
 "exp": 1426630228,"iat": 1426629028,
 "jti": "IDa64e5b0bba2b3dd363dadd1a2e695c103d615637c73d4ee103",
 "idpAccountId": "27658b82-5c5d-11e1-aebd-005056b10056",
 "idpEntityId": "pingidentity.com”, "attributes": … Omitted for brevity … ,
 "returnUrl":
   "https://sso.connect.pingidentity.com/sso/ppm/IDa64e5b0bba2b3dd363dadd1a2e695c103d615637c73d4ee103/",
 "dst": "https://authenticator.pingone.com/pingid/ppm/auth"
}
```

a request

```
{
 "iss": "pingidauthenticator",
 "sub": "bcampbell",
 "aud": "pingone",
 "nonce": "IDa64e5b0bba2b3dd363dadd1a2e695c103d615637c73d4ee103",
 "exp": 1426629341, "iat": 1426629041,
 "jti": "7MFL42RHR7DZY===",
 "status": "success",
 "idpAccountId": "27658b82-5c5d-11e1-aebd-005056b10056",
 "authnContext": "urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony",
 "inResponseTo": "IDa64e5b0bba2b3dd363dadd1a2e695c103d615637c73d4ee103",
 "dst":
     "https://sso.connect.pingidentity.com/sso/ppm/IDa64e5b0bba2b3dd363dadd1a2e695c103d615637c73d4ee103/"
}
```

& response

Next Steps?

- Please read https://tools.ietf.org/html/draft-campbell-oauth-dst4jwt-00
  - It's short! < 4 pages. <1 page if you skip the boilerplate, IANA claim registration, references, etc.
- I'd like to standardize it
  - it's useful for some applications
  - JWT Claims Registry is 'Specification Required'
- As WG document?
- Some other forum?

Thanks!

and remember…

can prevent malicious forwarding and redirection of JWTs

Brian Campbell
IETF #92
Dallas
March 2015