

OAuth is DAC. What do you
do for MAC?

About me

- Software architect
- Founder of secappdev.org
- Consultancy
- MVPs, PoCs, pilots
- Lecturer at EhB

<https://www.johanpeeters.com>



[@YoPeeters](https://twitter.com/YoPeeters)



yo@johanpeeters.com



OIDC rules the web

developers are disenchanted with SAML

affiliated to SOAP and WSDL

verbose and complex

OAuth is for authZ, not authN

authorization server vendors currently implement OAuth

OAuth authorization servers also support OAuth - buy one, get one for free

DAC vs MAC

OAuth gives end users control over clients' access to the resources they 'own'

businesses want control over data they hold, regardless of 'ownership'

in other words, they want MAC

they are familiar with RBAC

∴ authorization server extensions to support MAC

authorization server extensions

emerging consensus?

roles

JWT

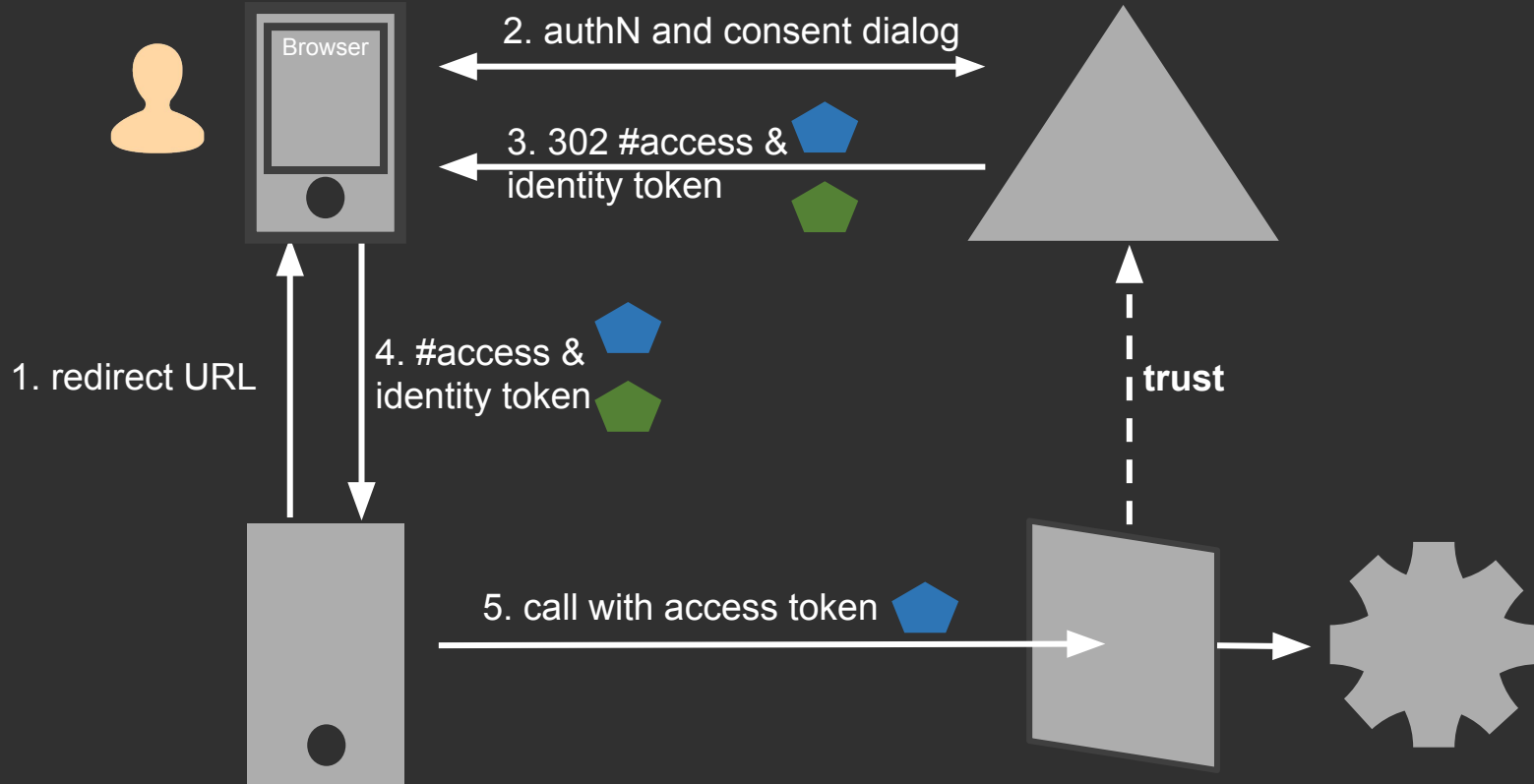
opportunities for leveraging existing constructs

scope

JWT

audience and authorized party

OpenID Connect Implicit Flow



Motion I: JWT as the access token format

OIDC specifies that the ID token must be a signed JWT

an ID token may contain several kinds of claims:

- standardized
 - mandatory
 - optional
- custom

OAuth does not standardize an access token format

JWT seems to be the emerging consensus for access tokens

but what claims should they contain?

Motion II: support RBAC

gigantic installed base

emerging consensus re. `roles` claim

roles are sets of permissions granted to the **end user**

Motion III: steal some of the ID token claims

aud

REQUIRED. Audience(s) that this ID Token is intended for. It MUST contain the OAuth 2.0 `client_id` of the Relying Party as an audience value. It MAY also contain identifiers for other audiences. ...

azp

OPTIONAL. Authorized party - the party to which the ID Token was issued. If present, it MUST contain the OAuth 2.0 Client ID of this party. This Claim is only needed when the ID Token has a single audience value and that audience is different than the authorized party. ...

acr

OPTIONAL. Authentication Context Class Reference. String specifying an Authentication Context Class Reference value that identifies the Authentication Context Class that the authentication performed satisfied. ...

Motion IV: syntax and semantics for scope token

OIDC defines scopes: openid, profile, email, address and phone

`<action>:<resource>` is often suggested for access token scope

- what actions? CRUD verbs?
- is resource related to URL? How?
- what impact on access token?
- what processing model in resource servers?
- what programming model in authorization servers?

References

OpenID Connect Core 1.0, https://openid.net/specs/openid-connect-core-1_0.html

JSON Web Token (JWT), <https://tools.ietf.org/html/rfc7519>

The OAuth 2.0 Authorization Framework, <https://tools.ietf.org/html/rfc6749>

Write-up of some of these issues, <https://t.co/hH1i9tXUQB>